MATA02 - The Magic of Numbers

TA: Angela Zavaleta-Bernuy
Tutorials: T2 (HW308 Thursdays 9-10am)
T3 (AA206 Tuesdays 9-10am)
T6 (MW160 Thursdays 10-11am)
Office hours: IC404 Mondays 2-4pm
email: angela.zavaletabernuy@mail.utoronto.ca
website: angelazb.github.io

Week 1 - Jan. 6th

No tutorials

Week 2 - Jan 13th

Today: Greatest Common Divisor (gcd) and Least Common Multiple (lcm)
↳ $\gcd(6,8) = 2$ ↳ $\text{lcm}(6,8) = 24$

Euclidean Algorithm: If $a = bq + r$, $0 \leq r < b$ then $\gcd(a,b) = \gcd(b,r)$

* $\gcd(a,0) = a$
* $\gcd(0,b) = b$
* $\text{lcm}(a,b) = \dfrac{ab}{\gcd(a,b)}$

Ex1: Use the Euclidean Algorithm to find $\gcd(51,96)$ and use it to find the $\text{lcm}(51,96)$

$96 = 51 \cdot 1 + 45$ → $d = \gcd(96,51)$

$51 = 45 \cdot 1 + 6$ → $d = \gcd(51,45)$

$45 = 6 \cdot 7 + 3$ → $d = \gcd(45,6)$

$6 = 3 \cdot 2 + 0$ ↳ stop! → $d = \gcd(6,3)$

$\therefore \gcd(96,51) = \gcd(51,45) = \gcd(45,6) = \gcd(6,3) = 3$

$\therefore \text{lcm}(96,51) = \dfrac{96 \times 51}{\gcd(96,51)} = \dfrac{96 \times 51}{3} = 96 \times 17 = 1632$

* If $a = ms$ and $b = mt$, then $\gcd(a,b) = m \times \gcd(s,t)$

Ex1: (Again!) but using this method.

$\gcd(51,96) = \gcd(3 \cdot 17, 3 \cdot 32) = 3 \cdot \gcd(17,32) = 3 \cdot 1 = 3$ ✓

Ex2: (T1-Q1) Use the Euclidean Algorithm to find gcd(366,150) and use it to find the lcm(366, 150)

$366 = 150 \cdot 2 + 66$ → $d = \gcd(366,150)$

$150 = 66 \cdot 2 + 18$ → $d = \gcd(150,66)$

$66 = 18 \cdot 3 + 12$ → $d = \gcd(66,18)$

$18 = 12 \cdot 1 + 6$ → $d = \gcd(18,12)$

$12 = 6 \cdot 2 + 0$ → $d = \gcd(12,6)$

$\therefore \gcd(366,150) = 6$

$\therefore \text{lcm}(366,150) = \frac{366 \times 150}{\gcd(366,150)} = \frac{366 \times 150}{6} = 61 \times 150 = 9150$

Ex3: (T1-Q3) Does the equation $12x + 20y = 90$ have a solution of integers x and y?

No :(Because on the left side we can factor out 4 → $4(3x+5y)$ however, 90 is not divisible by 4.

Ex4: Does the equation $11x + 1111 = 121 + 22y$ have a solution of integers x and y?

No :(Because the right side is divisible by 11 → $11(11+2y)$, but the left side isn't as 1111 is not divisible by 11.

Ex5: (T1-Q4) If a and b are integers, and x is an integer such that $x^2+ax+b = 0$. Show that $x \mid b$

↳ b is divisible by x

$x^2 + ax + b = 0$

$\Rightarrow b = -x^2 - ax$

$\Rightarrow b = -x(x+a)$

↳ is an integer because x and a are integers

Because b is also an integer, then $x \mid b$. ∎

Ex6: Show that if $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$

$a \mid b$ means that there exist an $n \in \mathbb{Z}$ such that $an = b$ ①

$b \mid a$ means that there exist an $m \in \mathbb{Z}$ such that $bm = a$ ②

Use ① for ②: $(an)m = a \Rightarrow anm = a \Rightarrow nm = 1$.

The only integers n and m that work for $nm=1$ are $n=m=1$ or $n=m=-1$

→ When $n=m=1 \Rightarrow a=b$, by ①

→ When $n=m=-1 \Rightarrow a=-b$, by ②

Week 3 - Jan 20th

Ex 1 (T2-Q1) Find integers x and y such that $6x+5y=4$

let's do Euclid's Algo!

$6 = 5 \cdot 1 + 1$ → But wait! This line here might help:

$5 = 1 \cdot 4 + 1$

$1 = 1 \cdot 1 + 0$

let's write it differently: $6 - 5 \cdot 1 = 1$

Now, we need the equation to equal 4: $(6 - 5 \cdot 1 = 1) \times 4$

$6 \cdot 4 - 5 \cdot 4 = 4$

The signs are different... $6 \cdot \underbrace{4}_{x} + 5 \cdot \underbrace{(-4)}_{y} = 4$

∴ In $6x+5y=4$, $x=4$, $y=-4$

Ex 2 Determine if the equations has integer solutions x and y.

eq 1 $1015x + 231y = 9$
eq 2 $1015x + 231y = 28$

① Find the gcd of (1015, 231)

$1015 = 231 \times 4 + 91$ (1)

$231 = 91 \times 2 + 49$ (2)

$91 = 49 \times 1 + 42$ (3)

$49 = 42 \times 1 + 7$ (4)

$42 = 7 \times 6 + 0$ → gcd (1015, 231) = 7

so by definition $\exists m, n$ such that $1015m + 231n = 7$

Looking at eq 1 and eq 2, $7 \nmid 9$ and $7 \mid 28$. So only eq 2 has integer solution.

② Write gcd in terms of the values.

$$
\begin{aligned}
7 &= 49 - 42\times 1 && (4)\\
&= 49 - (91 - 49\times 1) && (3)\\
&= 49\times 2 - 91\\
&= (231 - 91\times 2)\times 2 - 91 && (2)\\
&= 231\times 2 - 91\times 4 - 91\\
&= 231\times 2 - 91\times 5\\
&= 231\times 2 - (1015 - 231\times 4)\times 5 && (1)\\
&= 231\times 2 - 1015\times 5 + 231\times 20\\
7 &= 231\times 22 + 1015\times(-5)
\end{aligned}
$$

③ $4\times 7 = 231\times 22\times 4 + 1015\times(-5)\times 4$

$28 = 231\times \underbrace{88}_{y} + 1015\times \underbrace{(-20)}_{x}$

④ We want to find a general solution for $28 = 1015X + 231Y$

Theorem: If $d = \gcd(a,b) \mid c$ and x, y is an integer solution of $ax+by=c$, then so is $x + \frac{b}{d}t$, $y - \frac{a}{d}t$ for any integer t.

In this case, $d = 7 \mid 28$ and we have $28 = \underbrace{1015}_{a}x + \underbrace{231}_{b}y$
We know $x=-20$ and $y=88$ in ③

The general solution has $X = -20 + \frac{231}{7}t = -20 + 33t$

$Y = 88 - \frac{1015}{7}t = 88 - 145t$

∴ The general solution is $1015(-20+33t) + 231(88-145t) = 28$

Ex3 (T2-Q2) Find all integers x and y such that $30x + 8y = 500$. For which solutions are x and y both positive?

① $30 = 8\times 3 + 6$ (1)

$8 = 6\times 1 + 2$ (2)

$6 = 2\times 3 + 0$ → $\gcd(30, 8) = 2$

②
$$
\begin{aligned}
2 &= 8 - 6\times 1 && (2)\\
&= 8 - (30 - 8\times 3)\times 1 && (1)\\
&= 8 - 30\times 1 + 8\times 3\\
2 &= 8\times 4 + 30\times(-1)
\end{aligned}
$$

③ $250\times 2 = 8\times 4\times 250 + 30\times(-1)\times 250$

$500 = 8\times \underbrace{1000}_{y} + 30\times \underbrace{(-250)}_{x}$

④ General solution: $x = -250 + \frac{8}{2}t = -250 + 4t$

$y = 1000 - \frac{30}{2}t = 1000 - 15t$

$x \geq 0 \rightarrow -250 + 4t \geq 0$

$4t \geq 250$

$t \geq \frac{125}{2} = 62.5$

$y \geq 0 \rightarrow 1000 - 15t \geq 0$

$1000 \geq 15t$

$\frac{200}{3} \geq t \approx 66.\bar{6}$

So $62.5 \leq t \leq 66.\bar{6}$, t is an integer

$\therefore t = 63, 64, 65, 66$ to have x and y positive

Ex 4 (T2-Q4) Suppose the sophomores, juniors, and seniors in the tutorial decided to collect money to host a party. If each sophomore contributes \$25, each junior contributes \$18, each senior contributes \$10, \$450 will be collected. If there are 35 students, how many sophomores, juniors, and seniors are there?

$x + y + z = 35$ ①

$25x + 18y + 10z = 450$ ②

① $\times 10 \rightarrow 10x + 10y + 10z = 350$ ③

② $-$ ③ $\rightarrow 15x + 8y = 100$

let's do Euclid's Alg. to find the gcd of 15 and 8

① $15 = 8 \times 1 + 7$ (1)

$8 = 7 \times 1 + 1$ (2)

$7 = 1 \times 7 + 0$ $\rightarrow \gcd(15, 8) = 1$

② $1 = 8 - 7 \times 1$ (2)

$1 = 8 - (15 - 8 \times 1) \times 1$ (1)

$1 = 8 \times 2 - 15 \times 1$

$1 = 8 \times \underbrace{2}_{y} + 15 \times \underbrace{(-1)}_{x}$

↳ but there cannot be a negative solution!

③ $100 \times 1 = 8 \times 2 \times 100 + 15 \times (-1) \times 100$

$100 = 8 \times 200 + 15 \times (-100)$

④ General solution: $x = -100 + \frac{8t}{1} = -100 + 8t$

$y = 200 - \frac{15t}{1} = 200 - 15t$

We need to find $x \geq 0$, $y \geq 0$

$-100 + 8t \geq 0$

$8t \geq 100$

$t \geq \frac{25}{2} = 12.5$

$200 - 15t \geq 0$

$200 \geq 15t$

$13.\bar{3} \approx \frac{40}{3} \geq t$

$\Rightarrow 12.5 \leq t \leq 13.\bar{3}$, and t is an integer.

$\therefore t = 13 \rightarrow x = -100 + 8 \times 13 = -100 + 104 = 4$

$\rightarrow y = 200 - 15 \times 13 = 200 - 195 = 5$

$\rightarrow x + y + z = 35 \Rightarrow 4 + 5 + z = 35$

$\Rightarrow z = 26$

Ex 5 (T2-Q5) Show there are infinitely primes of the form $4t-1$, where t is an integer

Let's do a proof by contradiction. Which means, we will assume there are only a finite number of primes of the form $4t-1$, we will call them $p_1, p_2, \cdots, p_r$.

Let $N = p_1 p_2 \cdots p_r$, and let's consider the number $4N - 1$. By our initial assumption, $4N-1$ is not prime, so it has a prime factor!

We claim $4N-1$ has a prime factor of the form $4t-1$.

Now, let's see what happens when we multiply $4x+1$ and $4y+1$

$\rightarrow (4x+1)(4y+1) = 16xy + 4x + 4y + 1 = 4(4xy + x + y) + 1$

Which means, $4N-1$ must have a prime factor of form $4t-1$. Since 2 is not a factor.

So there is a p_i such that $p_i \mid 4N-1$. Then as $p_i \mid N$, we have $p_i \mid 1$. Which contradicts!

There are infinitely many primes of the form $4t-1$. ∎

Week 4 - Jan 27th

If n is composite, then it has a **prime divisor** p such that $p \leq \sqrt{n}$.

To determine if n is prime, check whether each of the prime numbers up to $\sqrt{n}$ divide n

Ex 1 (T3-Q1) Which of the following numbers are prime?

(a) 407

$\sqrt{407} < 21$ which means that we only need to check for primes up to 20

primes up to 20 $= \{2, 3, 5, 7, 11, 13, 17, 19\}$

- $2 \mid 407$? Nope! $407 = 2 \times 203 + 1$
- $3 \mid 407$? Nope! $407 = 3 \times 135 + 2$
- $5 \mid 407$? Nope! $407 = 5 \times 81 + 2$
- $7 \mid 407$? Nope! $407 = 7 \times 58 + 1$
- $11 \mid 407$? Yes $407 = 11 \times 37$

$\therefore$ 407 is not prime.

(b) 463

$\sqrt{463} < 22$ which means that we only need to check for primes up to 21

primes up to 21 $= \{2, 3, 5, 7, 11, 13, 17, 19\}$

- $2 \mid 463$? Nope! $463 = 2 \times 231 + 1$
- $3 \mid 463$? Nope! $463 = 3 \times 154 + 1$
- $5 \mid 463$? Nope! $463 = 5 \times 92 + 3$
- $7 \mid 463$? Nope! $463 = 7 \times 66 + 1$
- $11 \mid 463$? Nope! $463 = 11 \times 42 + 1$
- $13 \mid 463$? Nope! $463 = 13 \times 35 + 8$
- $17 \mid 463$? Nope! $463 = 17 \times 27 + 4$
- $19 \mid 463$? Nope! $463 = 19 \times 24 + 7$

$\therefore$ 463 is prime.

Sieve of Eratosthenes: To find all prime numbers between a and b ($a \leq b$), for each prime p up to $\sqrt{b}$, cross out every multiple of p. The remaining numbers are primes.

Ex2 Find all primes between 235 and 265

$\sqrt{265} < 17$ which means that we only need to check for primes up to 16

primes up to 16 = {2, 3, 5, 7, 11, 13}

~~235~~ ~~236~~ ~~237~~ ~~238~~ 239 ~~240~~ 241 ~~242~~ ~~243~~ ~~244~~

~~245~~ ~~246~~ ~~247~~ ~~248~~ ~~249~~ ~~250~~ 251 ~~252~~ ~~253~~ ~~254~~

~~255~~ ~~256~~ 257 ~~258~~ ~~259~~ ~~260~~ ~~261~~ ~~262~~ 263 ~~264~~

~~265~~

Step #1: Cross out all #s that are divisible by 2

Step #2: Cross out all #s that are divisible by 3

Step #3: Cross out all #s that are divisible by 5

Step #4: Cross out all #s that are divisible by 7

Step #5: Cross out all #s that are divisible by 11

Step #6: Cross out all #s that are divisible by 13

∴ The primes in between 235 and 265 are {239, 241, 251, 257, 263}

Ex3 (T3-Q2) Find all primes between 201 and 250

$\sqrt{250} < 16$ which means that we only need to check for primes up to 15

primes up to 15 = {2, 3, 5, 7, 11, 13}

~~201~~ ~~202~~ ~~203~~ ~~204~~ ~~205~~ ~~206~~ ~~207~~ ~~208~~ ~~209~~ ~~210~~

211 ~~212~~ ~~213~~ ~~214~~ ~~215~~ ~~216~~ ~~217~~ ~~218~~ ~~219~~ ~~220~~

~~221~~ ~~222~~ 223 ~~224~~ ~~225~~ ~~226~~ 227 ~~228~~ 229 ~~230~~

~~231~~ ~~232~~ 233 ~~234~~ ~~235~~ ~~236~~ ~~237~~ ~~238~~ 239 ~~240~~

241 ~~242~~ ~~243~~ ~~244~~ ~~245~~ ~~246~~ ~~247~~ ~~248~~ ~~249~~ ~~250~~

∴ The primes in between 201 and 250 are {211, 223, 227, 229, 233, 239, 241}

Ex 4 (T3-Q3) Find the prime-power decomposition for each of the following.

(a) $437 = 19 \times 23$

(b) $709 = 709$

(c) $876 = 2^2 \times 3 \times 73$

* An element x of a set is called a **unit** if there exists an element y such that $xy = 1$

* An **irreducible** is a non-unit element of A whose only positive divisors are itself, units, and products of itself and units.

Ex: Can we write a # in two different products of irreducibles, $A = 3t+1$?
$\Rightarrow 100 = 4 \times 25 = 10 \times 10$

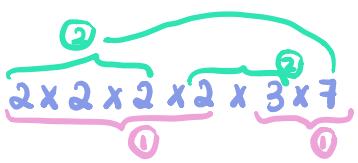
Ex 5 (T3-Q4) Consider the set containing positive integers of the form $5t+1$. Find an element of B with two different irreducible decompositions in B.

$t=1 \rightarrow 6 = 2 \times 3$
$t=2 \rightarrow 11 = 11$
$t=3 \rightarrow 16 = 2^4$
$t=4 \rightarrow 21 = 3 \times 7$
$t=5 \rightarrow 26 = 2 \times 13$
$t=6 \rightarrow 31 = 31$
$t=7 \rightarrow 36 = 2^2 \times 3^2$
$t=8 \rightarrow 41 = 41$
$t=9 \rightarrow 46 = 2 \times 23$
$t=10 \rightarrow 51 = 3 \times 17$
$t=11 \rightarrow 56 = 2^3 \times 7$
$\vdots$

Any common factors? 2^4, 3, 7

$2^4 \times 3 \times 7 = 336 = 335 + 1 = 5 \times 67 + 1$

How can we decompose 336? Remember they need to be in B (5t+1 form)



$336 = 56 \times 6 = 16 \times 21$
→ both are irreducible.

Ex 5 (T3-Q5) Suppose n is composite, and let p be the smallest prime divisor of n. If $p > \sqrt[3]{n}$, show that n/p is prime.

Suppose n/p is not prime. Then $n/p = q \times r$ where $q, r \in \mathbb{Z}$. Since p is the smallest prime divisor of n, then $p \leq q$ and $p \leq r$.

$\Rightarrow n = pqr \geq p^3 > (\sqrt[3]{n})^3 = n$

$\hookrightarrow n > n$?! impossible!

$\therefore n/p$ is prime ∎

Week 5 - Feb 3rd

Ex 1 (T4-Q1) Find the prime factorization of the product of 4460 and 6146

4460	2
2230	2
1115	5
223	223
1	

→ Check: 7, 11, 13 because $< \sqrt{223}$

6146	2
3073	7
439	439
1	

← Check: 11, 13, 17, 19 because $\sqrt{439}$

So $4460 = 2^2 \times 5 \times 223$ and $6146 = 2 \times 7 \times 439$

$\Rightarrow 4460 \times 6146 = 2^2 \times 5 \times 223 \times 2 \times 7 \times 439$
$= 2^3 \times 5 \times 7 \times 223 \times 439.$

Ex 2 (T4-Q2) Which of the following is the square of a fraction?

(a) $\frac{3^2 \times 5^{(3)}}{2^6}$ → NO. odd exponent.

(b) $\frac{3^2 \times 2^2}{5^4 \times 7^8}$ Yes! $\left(\frac{3 \times 2}{5^2 \times 7^4}\right)^2$

(c) $\frac{3^6 \times 2}{7^2 \times 2^3}$ Yes! → $\left(\frac{3^3}{7 \times 2}\right)^2$

(d) $13^2 \times 3^4$ Yes! $(13 \times 3^2)^2$

Ex 3 (T4-Q3) Using prime factorizations, compute the gcd and lcm of 7200 and 4374.

7200	2
3600	2
1800	2
900	2
450	2
225	3
75	3
25	5
5	5
1	

4374	2
2187	3
729	3
243	3
81	3
27	3
9	3
3	3
1	

→ $7200 = 2 \times 2 \times 2 \times 2 \times 2 \times 3 \times 3 \times 5 \times 5$
$= 2^5 \times 3^2 \times 5^2$

→ $4374 = 2 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3 \times 3$
$= 2 \times 3^7$

For the gcd, we will consider the common prime factors and smallest exponents.

$7200 = 2^5 \times 3^2 \times 5^2$ $\quad$ $4374 = 2 \times 3^7$

$\Rightarrow \gcd(7200, 4374) = 2 \times 3^2$

For the lcm, we will consider all prime factors and biggest exponents.

$7200 = 2^5 \times 3^2 \times 5^2$ $\quad$ $4374 = 2 \times 3^7$

$\Rightarrow \text{lcm}(7200, 4374) = 2^5 \times 3^7 \times 5^2$

Euler's Number: $\phi(n)$ to get the number of numbers from 1 to n that are relatively prime.

* If p is prime, then $\phi(p) = p - 1$
* If p is prime, then $\phi(p^n) = (p-1)p^{n-1}$
* If m and n are relatively prime, then $\phi(mn) = \phi(m)\phi(n)$
* Let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n, then $\phi(n) = n \times \frac{p_1 - 1}{p_1} \times \cdots \times \frac{p_r - 1}{p_r}$

Ex 4 Calculate the following:

(a) $\phi(48) = \phi(2^4 \times 3) = 48 \times \frac{2-1}{2} \times \frac{3-1}{3} = 2^4 \times 3 \times \frac{1}{2} \times \frac{2}{3} = 2^4 = 16$

(b) $\phi(480) = \phi(2^5 \times 3 \times 5) = 480 \times \frac{2-1}{2} \times \frac{3-1}{3} \times \frac{5-1}{5} = 2^5 \times 3 \times 5 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 2^7 = 128$

(c) $\phi(4800) = \phi(2^6 \times 3 \times 5^2) = 4800 \times \frac{2-1}{2} \times \frac{3-1}{3} \times \frac{5-1}{5} = 2^6 \times 3 \times 5^2 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 2^8 \times 5 = 1280$

(d) $\phi(55) = \phi(5 \times 11) = \phi(5) \times \phi(11) = (5-1)(11-1) = 4 \times 10 = 40$

$= 55 \times \frac{5-1}{5} \times \frac{11-1}{11} = 5 \times 11 \times \frac{4}{5} \times \frac{10}{11} = 40$

(e) $\phi(89) = 89 - 1 = 88$

(f) $\phi(32) = \phi(2^5) = (2-1)2^{5-1} = 2^4 = 16$

Ex 5 (T4-Q5) Find four values of n such that $\phi(n) = 8 = 2^3$

Remember $\phi(2^k) = 2^{k-1}$, $\phi(3) = 2$, $\phi(5) = 4 = 2^2$

Then for $\phi(n)=8$, $\phi(2^4)=2^3 \rightarrow \phi(16)$

$\phi(3)\phi(5)=8 \rightarrow \phi(15)$

$\phi(3)\phi(2^3)=8 \rightarrow \phi(24)$

$\phi(2^2)\phi(5)=8 \rightarrow \phi(20)$

$\therefore \phi(16)=\phi(15)=\phi(24)=\phi(20)=8$.

Week 6 - Feb 10th

Ex1 (T5-Q1) Calculate the following:

(a) How many numbers between 1 and 287 are <u>not</u> multiples of 7 or 41?

Way ①:

- Multiples of 7 between 1 and 287 : $\frac{287}{7}=41$
- Multiples of 41 between 1 and 287 : $\frac{287}{41}=7$
- Multiples of 7 and 41 between 1 and 287 : $\frac{287}{7\times 41}=1$

$\Rightarrow 287 - 41 - 7 + 1 = 240$

(287: total #s between 1 and 287; 41: mults of 7; 7: mults of 41; 1: mults of both 7 and 41)

Way ②: ONLY because $287=7\times 41$ and $\gcd(7,41)=1$, the numbers that are not multiples of 7 or 41 are numbers relatively prime to 287.

$\Rightarrow \phi(287)=\phi(7\times 41)=\phi(7)\phi(41)=(7-1)(41-1)=6\times 40=240$

$\therefore$ There are 240 numbers between 1 and 287 that are not multiples of 7 or 41.

(b) How many numbers between 1 and 363 are <u>not</u> multiples of 3 or 11?

Way ①:

- Multiples of 3 between 1 and 363 : $\frac{363}{3}=121$
- Multiples of 11 between 1 and 363 : $\frac{363}{11}=33$
- Multiples of 3 and 11 between 1 and 363 : $\frac{363}{3\times 11}=11$

$\Rightarrow 363 - 121 - 33 + 11 = 220$

Way ②: ONLY because $363 = 3 \times 11^2$ and $\gcd(3, 11) = 1$, the numbers that are not multiples of 3 or 11 are numbers relatively prime to 363

$\Rightarrow \phi(363) = \phi(3 \times 11^2) = \phi(3)\,\phi(11^2) = (3-1)(11-1)11 = 2 \times 10 \times 11 = 220$

$\therefore$ There are 220 numbers between 1 and 363 that are not multiples of 3 or 11.

(c) How many numbers between 1 and 78 are <u>not</u> multiples of 2, 3 or 13?

Way ①:

- Multiples of 2 between 1 and 78: $\frac{78}{2} = 39$
- Multiples of 3 between 1 and 78: $\frac{78}{3} = 26$
- Multiples of 13 between 1 and 78: $\frac{78}{13} = 6$
- Multiples of 2 and 3 between 1 and 78: $\frac{78}{2 \times 3} = 13$
- Multiples of 2 and 13 between 1 and 78: $\frac{78}{2 \times 13} = 3$
- Multiples of 3 and 13 between 1 and 78: $\frac{78}{3 \times 13} = 2$
- Multiples of 2, 3 and 13 between 1 and 78: $\frac{78}{2 \times 3 \times 13} = 1$

$\Rightarrow 78 - 39 - 26 - 6 + 13 + 3 + 2 - 1 = 24$

78: total #s between 1 and 78; 39: mults of 2; 26: mults of 3; 6: mults of 13; 13: mults of both 2 and 3; 3: mults of both 2 and 13; 2: mults of both 3 and 13; 1: mults of 2, 3 and 13

Way ②: ONLY because $78 = 2 \times 3 \times 13$ and 2, 3, and 13 are primes, the numbers that are not multiples of 2 or 3 or 13 are numbers relatively prime to 78

$\Rightarrow \phi(78) = \phi(2 \times 3 \times 13) = \phi(2)\,\phi(3)\,\phi(13) = (2-1)(3-1)(13-1) = 1 \times 2 \times 12 = 24$

$\therefore$ There are 24 numbers between 1 and 78 that are not multiples of 2, 3 or 13.

<u>Ex2</u> (T5-Q2) Calculate the following:

(a) How many numbers between 1 and 154 are <u>not</u> multiples of 7 or 11?

- Multiples of 7 between 1 and 154: $\frac{154}{7} = 22$

- Multiples of 11 between 1 and 154: $\frac{154}{11} = 14$
- Multiples of 7 and 11 between 1 and 154: $\frac{154}{7 \times 11} = 2$

$\Rightarrow 154 - 22 - 14 + 2 = 120$

$\therefore$ There are 120 numbers between 1 and 154 that are not multiples of 7 or 11.

Modular Arithmetic

$a+b$ in mod n is equal to the remainder of $a+b$ after dividing by n.

i.e. $a \equiv b \pmod{n}$ when $n \mid (a-b)$

Ex3 Calculate the following:

(a) $2+5 \pmod 4 \rightarrow 2+5 \equiv 3 \pmod 4$

(b) $15+13 \pmod{16} \rightarrow 15+13 \equiv 12 \pmod{16}$

(c) $22+8 \pmod{29} \rightarrow 22+8 \equiv 1 \pmod{29}$

(d) $21+8 \pmod{29} \rightarrow 21+8 \equiv 0 \pmod{29}$

Ex4 Make an addition table for mod 4 arithmetic

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

$3+1 = 2+2 = 1+3 = 4$
$\Rightarrow 4 \equiv 0 \bmod 4$

$3+2 = 2+3 = 5$
$\Rightarrow 5 \equiv 1 \bmod 4$

$3+3 = 6$
$\Rightarrow 6 \equiv 2 \bmod 4$

Ex5 (T5-Q4) Make an addition table for mod 9 arithmetic

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

Ex 6 (T5-Q5) Suppose today is Saturday. What day of the week will it be 200 days from now?

$200 \pmod 7 \equiv 4$ (7 days) or $200 \equiv 4 \bmod 7$

∴ It will be 4 days after Saturday (Wednesday)

Ex 7 Suppose we are in April. What month will it be 37 months from now?

$37 \pmod{12} \equiv 1$ (12 months) or $37 \equiv 1 \bmod 12$

∴ It will be 1 month after April (May)

Week 7 - Feb 17th

Reading week - No tutorial

Week 8 - Feb 24th

Ex 1 (T6-Q1) Calculate the following

(a) $-35 \pmod{80} \rightarrow -35 \equiv 80 - 35 \equiv 45 \pmod{80}$

(b) $-37 \pmod{42} \rightarrow -37 \equiv 42 - 37 \equiv 5 \pmod{42}$

Ex 2 (T6-Q2) Calculate the following

(a) $34 - 63 \pmod{73}$

Way ①: Change the numbers to their mod equivalent and then compute

$34 - 63 \equiv 34 + (-63) \equiv 34 + (73 - 63) \equiv 34 + 10 \equiv 44 \pmod{73}$

Way ②: Compute first and then find their mod equivalent.

$34 - 63 \equiv -29 \equiv 73 - 29 \equiv 44 \pmod{73}$

(b) $61 - 40 \pmod{71}$

Way ①: $61 - 40 \equiv 61 + (71 - 40) \equiv 61 + 31 \equiv 92 \equiv 21 \pmod{71}$

Way ②: $61 - 40 \equiv 21 \pmod{71}$

(c) $5 - 8 \pmod{75}$

Way ①: $5 - 8 \equiv 5 + (75 - 8) \equiv 5 + 67 \equiv 72 \pmod{75}$

Way ②: $5 - 8 \equiv -3 \equiv 72 \pmod{75}$

(d) $81-72 \pmod{85}$

Way ①: $81-72 \equiv 81+(85-72) \equiv 81+13 \equiv 94 \equiv 9 \pmod{85}$

Way ②: $81-72 \equiv 9 \pmod{85}$

Ex 3 (T6 - Q3) Calculate the following

(a) $3\times4 \pmod{88}$ → $3\times4 \equiv 12 \pmod{88}$

(c) $11\times14 \pmod{90}$ → $11\times14 \equiv 154 \equiv 64 \pmod{90}$

Ex 4 (T6-Q4) Calculate the following (Always show steps!)

(a) $8^2 \pmod{11}$

Way ①: $8^2 \equiv (8-11)^2 \equiv (-3)^2 \equiv 9 \pmod{11}$

Way ②: $8^2 \equiv 64 \equiv 9 \pmod{11}$

(b) $2^5 \pmod{12}$

$2^5 \equiv 32 \equiv 8 \pmod{12}$

(c) $9^9 \pmod{13}$

Way ①: $9^9 \equiv (-4)^9$ → is this any better? No :(

Way ②: $9^9 \equiv 9^8 9 \equiv (9^2)^4 9 \equiv (81)^4 9 \equiv 3^4 9 \equiv 81\times9 \equiv 3\times9 \equiv 27 \equiv 1 \pmod{13}$

($81 \equiv 3 \bmod 13$)

(d) $5^{12} \pmod{14}$

$5^{12} \equiv (5^2)^6 \equiv 25^6$ → $25 \equiv 11 \equiv -3 \pmod{14}$

Way ①: $\equiv 11^6 \equiv (11^2)^3 \equiv 121^3$ → $121 \equiv 9 \equiv -5 \pmod{14}$

*①A: $\equiv 9^3 \equiv 9^2\times9 \equiv 81\times9 \equiv 11\times9 \equiv 99 \equiv 1 \pmod{14}$ ($81 \equiv 11 \bmod 14$)

①B: $\equiv (-5)^3 \equiv (-5)^2\times(-5) \equiv 25\times(-5) \equiv 11\times(-5) \equiv -55 \equiv 1 \pmod{14}$

Way ②: $\equiv (-3)^6$

②A $\equiv (-3)^4(-3)^2 \equiv 81\times9 \equiv 11\times9 \equiv 99 \equiv 1 \pmod{14}$ ($81 \equiv 11 \bmod 14$)

②B $\equiv (-3)^3(-3)^3 \equiv (-27)(-27) \equiv (-1)(-1) \equiv 1 \pmod{14}$

Ex5 Make a multiplication table for mod 4 arithmetic

x	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$2 \times 2 \equiv 4 \equiv 0 \bmod 4$

$2 \times 3 \equiv 3 \times 2 \equiv 6 \equiv 2 \bmod 4$

$3 \times 3 \equiv 9 \equiv 1 \bmod 4$

Ex6 (T6-Q5) Make a multiplication table for mod 9 arithmetic

x	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

→ Symmetric?

Ex7 (T6-Q6) Suppose today is Sunday. What day of the week was it 150 days ago?

$150 = 7 \times 21 + 3 \qquad 150 \equiv 3 \pmod 7$

3 days ago from today (Sunday) → Thursday!

Ex8 (T6-Q7) Suppose you have 17 quarters and each package of M&Ms costs 95 cents. If you buy as many as possible, how much money will you have left over?

$75 \times 25 = 425$ cents or \$4.25

$425 = 95 \times 4 + 45 \qquad 425 \equiv 45 \pmod{95}$

You can get 4 packages and have \$0.45 left.

Week 9 - March 2nd

Ex1 (T6-Q1) Find the smallest nonnegative integer x such that

(a) $x \equiv 30 \pmod{13}$

$4 \equiv 30 \pmod{13} \rightarrow x = 4$

(b) $x \equiv -19 \pmod{13}$

$-6 \equiv 7 \pmod{13} \rightarrow x = 7$

Ex 2 (T7-Q2) Find the largest negative integer x s.t.

(a) $x \equiv 38 \bmod 42$

$38 - 42 \equiv -4 \pmod{42} \rightarrow x = -4$

(b) $x \equiv 40 \bmod 42$

$40 - 42 \equiv -2 \pmod{42} \rightarrow x = -2$

Ex 3 (T7-Q4) Compute the following:

(a) $27 \times 26 \pmod{29}$

$27 \times 26 \equiv (-2) \times (-3) \equiv 6 \pmod{29}$

(b) $45678904 \times 45678905 \pmod{45678903}$

$45678904 \times 45678905 \equiv (1) \times (2) \equiv 2 \pmod{45678903}$

(c) $85 \times 87 \pmod{86}$

$85 \times 87 \equiv (-1) \times (1) \equiv -1 \equiv 85 \pmod{86}$

(d) $71 \times 75 \pmod{73}$

$71 \times 75 \equiv (-2) \times (2) \equiv -4 \equiv 69 \pmod{73}$

(e) $35 \times 52 \pmod{16}$

$35 \times 52 \equiv 3 \times 4 \equiv 12 \pmod{16}$

(f) $3456782 \times 2145781 \pmod{3}$

3456780 is divisible by 3. Why? $(3+4+5+6+7+8+0) = 33 \rightarrow 3 \mid 33$.
2145780 is divisible by 3. Why? $(2+1+4+5+7+8+0) = 27 \rightarrow 3 \mid 27$

$(3456780+2) \times (2145780+1) \equiv (0+2) \times (0+1) \equiv 2 \pmod{3}$

Cancellation

If $ac \equiv bc \pmod{n}$ and $\gcd(c,n) = 1$, then $a \equiv b \pmod{n}$

If $ac \equiv bc \pmod{n}$ and $\gcd(c,n) = d$, then $a \equiv b \pmod{n/d}$

Ex 4 (T7-Q5) Solve the following:

(a) $3x \equiv 2 \pmod{16}$

$2 \equiv 18 \bmod 16 \rightarrow 3x \equiv 18 \pmod{16}$

Because $\gcd(3,16)=1$, $\frac{3}{3}x \equiv \frac{18}{3} \pmod{16}$

$\Rightarrow x \equiv 6 \pmod{16}$

(b) $5x \equiv 2 \pmod{16}$

$\underbrace{2 \equiv 18 \equiv 34 \equiv 50 \equiv 66}$ → $5x \equiv 50 \pmod{16}$

Find the divisible by 5 one

Because $\gcd(5,16)=1$, $\frac{5}{5}x \equiv \frac{50}{5} \pmod{16}$

$\Rightarrow x \equiv 10 \pmod{16}$

(c) $2x \equiv 4 \pmod{12}$

Because $\gcd(2,12)=2$, $\frac{2x}{2} \equiv \frac{4}{2} \pmod{\frac{12}{2}}$

$\Rightarrow x \equiv 2 \pmod{6}$

Ex 5 (T7-Q6) Prove that no integer of the form $9t+4$ is the sum of three cubes.

$\exists\, a,b,c$ s.t. $a^3+b^3+c^3 = 9t+4$

$\Rightarrow a^3+b^3+c^3 \equiv 4 \pmod{9}$

→ $0^3 \equiv 0 \pmod{9}$ → $3^3 \equiv 0 \pmod{9}$ → $6^3 \equiv 0 \pmod{9}$

→ $1^3 \equiv 1 \pmod{9}$ → $4^3 \equiv 1 \pmod{9}$ → $7^3 \equiv 1 \pmod{9}$

→ $2^3 \equiv 8 \pmod{9}$ → $5^3 \equiv 8 \pmod{9}$ → $8^3 \equiv 8 \pmod{9}$

So $x^3 \equiv 0, 1, 8 \pmod{9}$

There is no combination that will give 4. ▨

Week 10 - March 9th

Ex 1 (Q4-T8) Compute the following

(a) $6^{12} \pmod{22}$

$6^{12} \equiv (6^2)^6 \equiv (16^2)^2)^3 \pmod{22}$

$6^2 \equiv 36 \equiv 14 \equiv -8 \pmod{22}$
$6^4 \equiv (6^2)^2 \equiv (-8)^2 \equiv 64 \equiv 20 \equiv -2 \pmod{22}$

$\rightarrow 6^{12} \equiv (6^4)^3 \equiv (-2)^3 \equiv -8 \equiv 14 \pmod{22}$

(b) $10^8 \pmod{18}$

$10^2 \equiv 100 \equiv 10 \pmod{18}$
$10^4 \equiv (10^2)^2 \equiv 10^2 \equiv 100 \equiv 10 \pmod{18}$

$\rightarrow 10^8 \equiv (10^4)^2 \equiv 10^2 \equiv 100 \equiv 10 \pmod{18}$

Ex2 (Q1-T8) Compute the following:

(a) $\frac{1}{10} \pmod{13}$ Because $\gcd(10, 13) = 1$, $\frac{1}{10} \pmod{13}$ exists.

Way ① We need to find what # multiple of 10 has 1 mod 13

$10 \times 4 \equiv 40 \equiv 1 \bmod 13 \rightarrow \frac{1}{10} \equiv 4 \pmod{13}$

Way ② Euclidean Algo!

$13 = 10 \times 1 + 3$
$10 = 3 \times 3 + 1$

$1 = 10 - 3 \times 3$
$1 = 10 - (13 - 10 \times 1) \times 3$
$1 = 10 - 13 \times 3 + 10 \times 3$
$1 = 10 \times 4 - \underbrace{13 \times 3}$ divisible by 13

$1 \equiv 10 \times 4 \pmod{13}$
$\rightarrow \frac{1}{10} \equiv 4 \pmod{13}$

(c) $\frac{1}{40} \pmod{41}$ Because $\gcd(40, 41) = 1$, $\frac{1}{40} \pmod{41}$ exists.

$40 \equiv (-1) \bmod 40 \rightarrow (-1)(-1) \equiv 1 \equiv (40)(40) \pmod{41}$

$\rightarrow \frac{1}{40} \equiv 40 \pmod{41}$

(d) $\frac{1}{122} \pmod{501}$ Because $\gcd(122, 501) = 1$, $\frac{1}{122} \pmod{501}$ exists.

$501 = 122 \times 4 + 13$
$122 = 13 \times 9 + 5$
$13 = 5 \times 2 + 3$
$5 = 3 \times 1 + 2$
$3 = 2 \times 1 + 1$

$1 = 3 - 2 \times 1$
$= 3 - (5 - 3 \times 1) \times 1$
$= 3 - 5 + 3$
$= 3 \times 2 - 5$

$= (13-5\times2)\times2-5$
$= 13\times2-5\times5$
$= 13\times2-(122-13\times9)\times5$
$= 13\times2-122\times5+13\times45$
$= 13\times47-122\times5$
$= (501-122\times4)\times47-122\times5$
$= 501\times47-122\times188-122\times5$
$= 501\times47-122\times193$

$\rightarrow 1 \equiv 501\times47-122\times193 \equiv 122\times(-193) \equiv 122\times308 \pmod{501}$

$\frac{1}{122} \equiv 308 \pmod{501}$

(f) $\frac{4}{12} \pmod{41}$ Because $\gcd(12,41)=1$, $\frac{4}{12} \pmod{41}$ exists.

$41 = 12\times3+5$
$12 = 5\times2+2$ ← need to get to 4

$2 = 12-5\times2$
$= 12-(41-12\times3)\times2$
$= 12-41\times2+12\times6$
$(2 = 12\times7-41\times2)\times2$

$4 = 12\times14-41\times4$

$\rightarrow 4 \equiv 12\times14-41\times4 \equiv 12\times14 \pmod{41}$

$\therefore \frac{4}{12} \equiv 14 \pmod{41}$

Ex3 (Q2-T8) Solve the following

(a) $2x \equiv 3 \pmod{21}$ $\gcd(2,21)=1 \rightarrow \frac{1}{2} \pmod{21}$ exists.

$1 \equiv 22 \pmod{21} \rightarrow \frac{1}{2} \equiv 11 \pmod{21}$

$x \equiv 3\times11 \equiv 33 \equiv 12 \pmod{21}$

(b) $6\frac{x}{3} \equiv \frac{9}{3} \pmod{\frac{21}{3}}$ $\gcd(6,21)=3$, so we need to use cancellation

$\rightarrow 2x \equiv 3 \pmod{7}$ $\gcd(2,7)=1 \rightarrow \frac{1}{2} \bmod 7$ exists.

$1 \equiv 8 \pmod{7} \rightarrow 8 = 2\times4 \rightarrow \frac{1}{2} \equiv 4 \bmod 7$

$\rightarrow x \equiv 3\times4 \equiv 12 \equiv 5 \pmod{7}$

Ex4 (Q3-T8) Find all the reciprocals of non-zero values mod 13

If $\frac{1}{a} \equiv b$, then $\frac{1}{b} \equiv a$ and $\frac{1}{-a} \equiv -b$

$\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Want to find a pair of #s that multiplied together, its product is 1 mod 13

$1 \times 1 \equiv 1 \bmod 13$
$12 \times 12 \equiv 144 \equiv 1 \bmod 13$

$2 \times 7 \equiv 14 \equiv 1 \bmod 13$
$7 \times 2 \equiv 14 \equiv 1 \bmod 13$

$3 \times 9 \equiv 27 \equiv 1 \bmod 13$
$9 \times 3 \equiv 27 \equiv 1 \bmod 13$

$4 \times 10 \equiv 40 \equiv 1 \bmod 13$
$10 \times 4 \equiv 40 \equiv 1 \bmod 13$

$5 \times 8 \equiv 40 \equiv 1 \bmod 13$
$8 \times 5 \equiv 40 \equiv 1 \bmod 13$

$6 \times 11 \equiv 66 \equiv 1 \bmod 13$
$11 \times 6 \equiv 66 \equiv 1 \bmod 13$

x	1/x
1	1
2	7
3	9
4	10
5	8
6	11
7	2
8	5
9	3
10	4
11	6
12	12

Week 11 - March 16th

Fermat's Theorem: If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$.

Ex1 Compute the following

(a) $5^{(2)} \bmod 3$ → $3-1=2$

Checklist:
- ☐ Is p prime?
- ☐ $p \nmid a$?

Check:
- ✓ 3 is prime
- ✓ $3 \nmid 5$

} We can use Fermat's!

$\Rightarrow 5^2 \equiv 1 \bmod 3$

We could also solve it straight forward to check it works!

$5^2 \equiv 25 \equiv 1 \bmod 3 \rightarrow 25 = 3\times 8 + 1$ ☺

(b) (T9-Q1) $16^{28} \bmod 29$

$28 \rightarrow 29-1$

Check:
✓ 29 is prime
✓ $29 \nmid 16$

By Fermat's Theorem,

$16^{28} \equiv 1 \bmod 29$

(c) (T9-Q1) $14^{10} \bmod 5$

$10-1=9 \neq$ oh no...

Check:
✓ 5 is prime
✓ $5 \nmid 14$

} This tells us we can use Fermat's Theorem, but the exponent of 14 is NOT 5-1. Now what?!

Well: $14^{10} \equiv (14^4)^2\, 14^2$

14^4 → found it! now we can compute everything separate.

$\Rightarrow 14^4 \equiv 1 \bmod 5$, by Fermat's Theorem

$\Rightarrow 14 \equiv 4 \equiv -1 \bmod 5$

$\therefore 14^{10} \equiv (14^4)^2 14^2 \equiv (1)^2(-1)^2 \equiv 1 \bmod 5$

(d) (T9-Q1) $7^{436} \bmod 5$

Check:
✓ 5 is prime
✓ $5 \nmid 7$

} We can use Fermat's but we need to find a way to bring 7^4 in.

$7^{436} \equiv (7^4)^{109} \equiv 1^{109} \equiv 1 \bmod 5$, by Fermat's Theorem.

(e) (T9-Q1) $5^{251} \bmod 7$

Check:
✓ 7 is prime
✓ $7 \nmid 5$

} We can use Fermat's but we need to find a way to bring 5^6 in.

Let's do some division! $251 = 6\times 41 + 5 \Rightarrow 5^{251} \equiv (5^6)^{41} \times 5^5$

$\Rightarrow 5^6 \equiv 1 \bmod 7$, by Fermat's Theorem.

$\Rightarrow 5^5 \equiv 5^4 5 \equiv (-2)^4 5 \equiv 16\times 5 \equiv 2\times 5 \equiv 10 \equiv 3 \bmod 7$

$\therefore 5^{251} \equiv (5^6)^{41} \times 5^5 \equiv (1)^{41} \times 3 \equiv 3 \bmod 7$

Ex2 (T9-Q2) Use the Mod 7 Power table below, find all solutions to the following:

b	1	2	3	4	5	6
1^b	1	1	1	1	1	1
2^b	2	4	1	2	4	1
3^b	3	2	6	4	5	1
4^b	4	2	1	4	2	1
5^b	5	4	6	2	3	1
6^b	6	1	6	1	6	1

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

Look at all cubes: this col.
None give you 5.

(b) $x^4 \equiv 2 \pmod 7$

Look at this col:
Two values give you 2: 2, 5

(c) $x^5 \equiv 1 \pmod 7$

Look at this col.
1 gives you 1

(d) $x^5 \equiv 4 \pmod 7$

Look at this col.
2 gives you 4

Modular Roots: We say a is k-th root of $b \pmod n$ if $a^k \equiv b \pmod n$

Unique Roots: Let p be a prime. If $\gcd(k, p-1) = 1$, then the equation $x^k \equiv b \pmod p$ has exactly one solution. If $\gcd(k, p-1) \neq 1$, then the equation $x^k \equiv b \pmod p$ has either no solution or multiple solutions.

If $\gcd(k, p-1) = 1$, then $x^k \equiv b \pmod p$ has solution b^y, where y is the solution to $ky \equiv 1 \pmod{p-1}$

Ex3 (T9-Q4) Solve the following

(a) $x^9 \equiv 2 \pmod{17}$

① $\gcd(9, 16) = 1$: unique solution

We know $x^9 \equiv 2 \pmod{17}$ has a solution 2^y where y is the solution of $9y \equiv 1 \pmod{16}$

② Solve $9y \equiv 1 \pmod{16}$

Euclidean:
$16 = 9 \times 1 + 7$
$9 = 7 \times 1 + 2$
$7 = 2 \times 3 + 1$

$1 = 7 - 2 \times 3$
$1 = 7 - (9 - 7 \times 1) \times 3$
$1 = 7 \times 4 - 9 \times 3$
$1 = (16 - 9 \times 1) \times 4 - 9 \times 3$
$1 = 16 \times 4 + 9 \times (-7)$

$\Rightarrow 9(-7) \equiv 1 \pmod{16}$ $\Rightarrow 9(-7) \equiv 9\times(16-7) \equiv 9\times 9 \equiv 1 \pmod{16}$

$\Rightarrow y = 9$

③ Solve $2^y = 2^9$ which is the solution of $x^9 \equiv 2 \pmod{17}$

i.e. Solve $2^9 \bmod 17$

$2^9 \equiv (2^4)^2\, 2 \equiv (16)^2 2 \equiv (-1)^2(2) \equiv 2 \bmod 17$

(b) $x^5 \equiv 3 \pmod{47}$

① $\gcd(5,46) = 1$: unique solution

We know $x^5 \equiv 3 \pmod{47}$ has a solution 3^y where y is the solution of $5y \equiv 1 \pmod{46}$

② Solve $5y \equiv 1 \pmod{46}$

Euclidean: $46 = 5\times 9 + 1 \rightarrow 1 = 46 - 5\times 9$

$1 = 46 + 5\times(-9)$

$\Rightarrow 5\times(-9) \equiv 1 \pmod{46}$ $\Rightarrow 5\times(-9) \equiv 5\times(46-9) \equiv 5\times 37 \equiv 1 \bmod 46$

$\Rightarrow y = 37$

③ Solve $3^y = 3^{37}$ which is the solution of $x^5 \equiv 3 \pmod{47}$

i.e. Solve $3^{37} \bmod 47$

$3^{37} \equiv 3^{36}\, 3 \equiv 3^{32}\, 3^4\, 3 \pmod{47}$

$3^2 \equiv 9 \bmod 47$
$3^4 \equiv 81 \equiv 34 \equiv -13 \bmod 47$
$3^8 \equiv (3^4)^2 \equiv (-13)^2 \equiv 169 \equiv 28 \equiv -19 \bmod 47$
$3^{16} \equiv (3^8)^2 \equiv (-19)^2 \equiv 361 \equiv 32 \equiv -15 \bmod 47$
$3^{32} \equiv (3^{16})^2 \equiv (-15)^2 \equiv 225 \equiv 37 \equiv -10 \bmod 47$

$\Rightarrow 3^{37} \equiv 3^{32}\, 3^4\, 3 \equiv (-10)(-13)(3) \equiv (130)(3) \equiv (36)(3) \equiv 108 \equiv 14 \pmod{47}$

Week 12 - March 23rd

Euler's Theorem: Let n be a positive integer. If n and a are relatively prime, then $a^{\phi(n)} \equiv 1 \bmod n$

Ex 1 Compute the following:

(a) (T10-Q1) $3^{20} \pmod{25}$

Checklist:
☑ gcd(n,a)=1? gcd(25,3)=1
☑ Ø(n)? Ø(25) = Ø(5²) = 5^(2-1)(5-1) = 5x4 = 20 → exponent of 3!

By Euler's Thm, $3^{20} \equiv 3^{\emptyset(25)} \equiv 1 \bmod 25$

(b) $4^{18} \pmod{27}$

Checklist:
☑ gcd(n,a)=1? gcd(27,4)=1
☑ Ø(n)? Ø(27) = Ø(3³) = 3^(3-1)(3-1) = 9x2 = 18 → exponent of 4!

By Euler's Thm, $4^{18} \equiv 4^{\emptyset(27)} \equiv 1 \bmod 27$

(c) $9^{780} \bmod 7$

* Check:
✓ 7 is prime
✓ 7 ∤ 9
} We can use Fermat's but we need to find a way to bring 9^6 in.

$9^{780} \equiv (9^6)^{130} \equiv 1^{130} \equiv 1 \bmod 7$, by Fermat's Theorem

* Checklist:
☑ gcd(7,9)=1?
☑ Ø(7)? Ø(7) = 7-1 = 6 → 780 = 130 x 6

$\Rightarrow 9^6 \equiv 9^{\emptyset(7)} \equiv 1 \bmod 7$

By Euler's Thm, $9^{780} \equiv (9^6)^{130} \equiv (1)^{130} \equiv 1 \bmod 7$

(d) (T9-Q1) $7^{436} \bmod 5$

* Check:
✓ 5 is prime
✓ 5 ∤ 7
} We can use Fermat's but we need to find a way to bring 7^4 in.

$7^{436} \equiv (7^4)^{109} \equiv 1^{109} \equiv 1 \bmod 5$, by Fermat's Theorem.

* Checklist:
☑ gcd(5,7)=1?
☑ Ø(5)? Ø(5) = 5-1 = 4 → 436 = 109 x 4

$\Rightarrow 7^4 \equiv 7^{\emptyset(5)} \equiv 1 \bmod 5$

By Euler's Thm, $7^{436} \equiv (7^4)^{109} \equiv (1)^{109} \equiv 1 \bmod 5$

★ If a and n are relatively prime, $a^{\emptyset(n)} \equiv 1 \pmod n$, so if m divides Ø(n) with remainder r, then $a^m \equiv a^r \pmod n$

(e) (T10-Q1) $5^{19} \pmod{28}$

Checklist:
☑ gcd(28,5)=1?
☑ Ø(28)? $\quad Ø(28) = Ø(2^2 \times 7) = Ø(2^2)\,Ø(7) = 2 \times 6 = 12$

⇒ Do the division algorithm with Ø(28)=12 and 19

$19 = 12 \times 1 + \underset{r}{7} \rightarrow * \quad 5^{19} \equiv 5^7 \pmod{28}$

By Euler's Thm, $\quad 5^{19} \equiv 5^7 \equiv 5^6 \times 5 \equiv 1 \times 5 \equiv 5 \bmod 28$ //

· $5^6 \equiv (5^2)^3 \equiv (25)^3 \equiv (-3)^3 \equiv -27 \equiv 1 \bmod 28$

(f) (T10-Q1) $4^{386} \pmod{51}$

Checklist:
☑ gcd(51,4)=1?
☑ Ø(51)? $\quad Ø(51) = Ø(3 \times 17) = Ø(3) \times Ø(17) = 2 \times 16 = 32$

⇒ Do the division algorithm with Ø(51)=32 and 386

$386 = 32 \times 12 + \underset{r}{2} \rightarrow * \quad 4^{386} \equiv 4^2 \pmod{51}$

By Euler's Thm, $\quad 4^{386} \equiv 4^2 \equiv 16 \pmod{51}$ //

Unique Roots: If $\gcd(k, Ø(n)) = 1$ and $\gcd(b,n) = 1$, then the equation $x^k \equiv b \pmod n$ has exactly one solution.

If $\gcd(k, Ø(n)) = 1$ and $\gcd(b,n) = 1$, then the equation $x^k \equiv b \pmod n$ has solution b^y, where y is the solution to $ky \equiv 1 \pmod{Ø(n)}$

Ex2 (T10-Q3) Which of the following have a unique sol?

(a) $x^3 \equiv 5 \pmod{18}$

$k=3,\ b=5,\ n=18$

$Ø(18) = Ø(2 \times 3^2) = Ø(2) \times Ø(3^2) = (2-1)\,3^1\,(3-1) = 6$

① $\gcd(3,6) = 3 \neq 1$ and $\gcd(5,18) = 1$ ⇒ not unique solution!

(b) $x^4 \equiv 6 \pmod{18}$

$k=4,\ b=6,\ n=18$

$Ø(18) = Ø(2 \times 3^2) = Ø(2) \times Ø(3^2) = (2-1)\,3^1\,(3-1) = 6$

① $\gcd(4,6) = 2 \neq 1$ and $\gcd(6,18) = 6 \neq 1$ ⇒ not unique solution!

(c) $x^5 \equiv 7 \pmod{18}$

$k=5$, $b=7$, $n=18$, $\phi(18)=6$

① $\gcd(5,6)=1$ and $\gcd(7,18)=1$ => unique solution!

We know $x^5 \equiv 7 \pmod{18}$ has a solution 7^y where y is the solution of $5y \equiv 1 \pmod{6}$

② Solve $5y \equiv 1 \pmod{6}$

$6 = 5 \times 1 + 1 \rightarrow 1 = 6 - 5 \times 1$

$1 = 6 \times 1 + 5 \times (-1)$

$\Rightarrow 5 \times (-1) \equiv 5 \times 5 \equiv 25 \equiv 1 \pmod{6}$

$\rightarrow y = 5$

③ Solve $7^y = 7^5$ which is the solution of $x^5 \equiv 7 \pmod{18}$

i.e. Solve $7^5 \bmod 18$

$7^2 \equiv 49 \equiv 13 \equiv -5 \pmod{18}$

$7^4 \equiv (7^2)^2 \equiv (-5)^2 \equiv 25 \equiv 7 \pmod{18}$

$\Rightarrow 7^5 \equiv 7^4 \times 7 \equiv 7 \times 7 \equiv 13 \pmod{18}$ ie. $x = 13 \pmod{18}$

(d) $x^5 \equiv 5 \pmod{18}$

$k=5$, $b=5$, $n=18$, $\phi(18)=6$

① $\gcd(5,6)=1$ and $\gcd(5,18)=1$ => unique solution!

We know $x^5 \equiv 5 \pmod{18}$ has a solution 5^y where y is the solution of $5y \equiv 1 \pmod{6}$

② Solve $5y \equiv 1 \pmod{6}$

$6 = 5 \times 1 + 1 \rightarrow 1 = 6 - 5 \times 1$

$1 = 6 \times 1 + 5 \times (-1)$

$\Rightarrow 5 \times (-1) \equiv 5 \times 5 \equiv 25 \equiv 1 \pmod{6}$

$\rightarrow y = 5$

③ Solve $5^y = 5^5$ which is the solution of $x^5 \equiv 5 \pmod{18}$

i.e. Solve $5^5 \bmod 18$

$5^2 \equiv 25 \equiv 7 \pmod{18}$
$5^4 \equiv (5^2)^2 \equiv 7^2 \equiv 49 \equiv 13 \pmod{18}$

$\Rightarrow 5^5 \equiv 5^4 \times 5 \equiv 13 \times 5 \equiv 65 \equiv 11 \pmod{18}$ ie. $x = 11 \pmod{18}$

Week 13 - March 30th

Ex1 (T11 - Q1) Solve the following:

(a) $x^3 \equiv 5 \pmod{16}$

$k=3,\ b=5,\ n=16,\ \phi(16) = \phi(2^4) = 2^3(2-1) = 8$

① Check: $\gcd(k, \phi(n)) = \gcd(3,8) = 1$
$\gcd(b, n) = \gcd(5,16) = 1$
} a unique solution exists!

We know $x^3 \equiv 5 \pmod{16}$ has a solution 5^y, where y is the solution of $3y \equiv 1 \bmod 8$

② Solve $3y \equiv 1 \bmod 8$

$8 = 3 \times 2 + 2$
$3 = 2 \times 1 + 1$

$\rightarrow 1 = 3 - 2 \times 1$
$1 = 3 - (8 - 3 \times 2) \times 1$
$1 = 3 - 8 \times 1 + 3 \times 2$
$1 = 3 \times 3 + 8 \times (-1)$

$\Rightarrow y = 3$

③ Solve $5^y = 5^3$ which is the solution of $x^3 \equiv 5 \bmod 16$

i.e. Solve $5^3 \bmod 16$

$5^2 \equiv 25 \equiv 9 \bmod 16$
$5^3 \equiv 5 \times 5^2 \equiv 5 \times 9 \equiv 45 \equiv 13 \bmod 16$

$\Rightarrow x = 13 \bmod 16$

(b) $x^7 \equiv 3 \pmod{25}$

$k=7,\ b=3,\ n=25,\ \phi(25) = \phi(5^2) = (5-1)5 = 20$

① Check: $\gcd(k, \phi(n)) = \gcd(7,20) = 1$
$\gcd(b, n) = \gcd(3,25) = 1$
} a unique solution exists!

We know $x^7 \equiv 3 \pmod{25}$ has a solution 3^y, where y is the solution of $7y \equiv 1 \bmod 20$

② Solve $7y \equiv 1 \bmod 20$

$20 = 7\times 2 + 6$ → $1 = 7 - 6\times 1$

$7 = 6\times 1 + 1$ → $1 = 7 - (20 - 7\times 2)\times 1$

$1 = 20\times(-1) + 7\times 3$

$\Rightarrow y = 3$

③ Solve $3^3 = 3^3$ which is the solution of $x^7 \equiv 3 \pmod{25}$

i.e. Solve $3^3 \bmod 25$

$3^3 \equiv 27 \equiv 2 \bmod 25$

$\Rightarrow x \equiv 2 \bmod 25$

The **order** of $x \pmod n$ is the smallest positive integer t such that $x^t \equiv 1 \bmod n$

⇒ Suppose that $\gcd(a,n) = 1$ and a has order $t \pmod n$. Then $t \mid \phi(n)$

Ex 2 Find the order of $1, 2, 3, 4 \pmod 5$

* $1^1 \equiv 1 \bmod 5 \quad \Rightarrow t = 1$

* $2 \not\equiv 1 \bmod 5$

  $2^2 \equiv 4 \not\equiv 1 \bmod 5$

  $2^3 \equiv 8 \not\equiv 1 \bmod 5$

  $2^4 \equiv 16 \equiv 1 \bmod 5 \Rightarrow t = 4$

* $3 \not\equiv 1 \bmod 5$

  $3^2 \equiv 9 \not\equiv 1 \bmod 5$

  $3^3 \equiv 27 \not\equiv 1 \bmod 5$

  $3^4 \equiv 81 \equiv 1 \bmod 5 \Rightarrow t = 4$

* $4 \not\equiv 1 \bmod 5$

  $4^2 \equiv 16 \equiv 1 \bmod 5 \Rightarrow t = 2$

∴ 1 has order 1, 2 has order 4, 3 has order 4 and 4 has order 2 $\pmod 5$

If a is a least residue and the order $a \pmod n$ is $\phi(n)$, then a is called a **primitive root** of n.

⇒ Suppose that a has order $t \pmod n$. Then a^k has order t if and only if $\gcd(k,t)=1$

Ex3 Find the primitive roots.

(a) (T11- Q3) One of the primitive roots of 17 is 3. Find all the others.

i.e. $\phi(17)=16$ so $3^{16} \equiv 1 \bmod 17$
So all the other primitives are of the form 3^t where $\gcd(t,16)=1$

$\Rightarrow t = 1, 3, 5, 7, 9, 11, 13, 15$

* $3^1 \equiv 3 \bmod 17$
* $3^3 \equiv 27 \equiv 10 \bmod 17$
* $3^5 \equiv 3^3 \times 3^2 \equiv 10 \times 9 \equiv 90 \equiv 5 \bmod 17$
* $3^7 \equiv 3^5 \times 3^2 \equiv 5 \times 9 \equiv 45 \equiv 11 \bmod 17$
* $3^9 \equiv 3^7 \times 3^2 \equiv 11 \times 9 \equiv 99 \equiv 14 \bmod 17$
* $3^{11} \equiv 3^9 \times 3^2 \equiv 14 \times 9 \equiv 126 \equiv 7 \bmod 17$
* $3^{13} \equiv 3^{11} \times 3^2 \equiv 7 \times 9 \equiv 63 \equiv 12 \bmod 17$
* $3^{15} \equiv 3^{13} \times 3^2 \equiv 12 \times 9 \equiv 108 \equiv 6 \bmod 17$

∴ The primitive roots of 17 are 3, 10, 5, 11, 14, 7, 12 and 6.

(b) One of the primitive roots of 13 is 2. Find all the others:

i.e. $\phi(13) = 13-1 = 12$ so $2^{12} \equiv 1 \bmod 13$
So all the other primitives are of the form 2^t where $\gcd(t,12)=1$

$\Rightarrow t = 1, 5, 7, 11$

* $2^1 \equiv 2 \bmod 13$
* $2^5 \equiv 2^4 \times 2 \equiv 16 \times 2 \equiv 3 \times 2 \equiv 6 \bmod 13$
* $2^7 \equiv 2^5 \times 2^2 \equiv 6 \times 4 \equiv 24 \equiv 11 \bmod 13$
* $2^{11} \equiv 2^7 \times 2^4 \equiv 11 \times 16 \equiv 11 \times 3 \equiv 33 \equiv 7 \bmod 13$

∴ The primitive roots of 13 are 2, 6, 11 and 7.

RSA Algorithm

1. Suppose Alice wants to send the number a to Bob
2. Bob picks two prime numbers p and q, calculates $N = p \times q$ and $\phi(N) = \phi(p \times q)\ \phi(p)\phi(q) = (p-1)(q-1)$, and chooses K relatively prime to $\phi(N)$
3. Bob publishes K and N and keeps p and q secret.
4. Alice calculates $b = a^K \pmod N$ and sends it (publicly) to Bob.
5. Bob solves $x^K \equiv b \pmod N$, and obtains the message.

Ex4 (T11-Q5) Suppose Alice wants to send Bob the secret number $a=4$ and Bob has provided $K=11$ and $N=183$. What is the encoded message that Alice should send Bob?

How to encrypt a message a, given K and N?

$\Rightarrow$ Calculate $a^K \bmod N$

$a^K = 4^{11} \bmod 183$

$\rightarrow 4^2 \equiv 16 \bmod 183$

$\rightarrow 4^4 \equiv (4^2)^2 \equiv 256 \equiv 73 \bmod 183$

$\rightarrow 4^8 \equiv (4^4)^2 \equiv 73^2 \equiv 5329 \equiv 22 \bmod 183$

$\Rightarrow 4^{11} \equiv 4^8 4^2 4 \equiv 22 \times 16 \times 4 \equiv 1408 \equiv 127 \bmod 183$

$\therefore$ encoded message $b = 127$

Ex5 (T11-Q6) Suppose that Alice has sent Bob the encoded message $b=9$ and Bob has chosen $p=5$ and $q=7$. If $K=19$, what is Alice's original message?

How to decrypt given b, p, q, and K.

$\Rightarrow$ Solve $x^K \equiv b \bmod N$, where $N = pq$.
$\Rightarrow$ $x^{19} \equiv 9 \bmod 35$

(*) We can use what we learnt last week!

$\phi(35) = \phi(7)\phi(5) = 6 \times 4 = 24$

① Check $\gcd(K, \phi(n)) = \gcd(19, 24) = 1$
$\gcd(b, n) = \gcd(9, 35) = 1$
} We can find a solution!

The solution for $x^{19} \equiv 9 \bmod 35$ is 9^y where y is the solution of $19y \equiv 1 \bmod 24$

② Solve $19y \equiv 1 \bmod 24$

$24 = 19\times1 + 5$
$19 = 5\times3 + 4$
$5 = 4\times1 + 1$

$\rightarrow$
$1 = 5 - 4\times1$
$1 = 5 - (19-5\times3)\times1$
$1 = 5 - 19\times1 + 5\times3$
$1 = 5\times4 - 19\times1$
$1 = (24 - 19\times1)\times4 - 19\times1$
$1 = 24\times4 - 19\times4 - 19\times1$
$1 = 24\times4 + 19\times(-5)$

$\rightarrow -5 \equiv 19 \bmod 24 \rightarrow y = 19$

③ The solution of $x^{19} \equiv 9 \bmod 35$ is $x = 9^{19}$
i.e. Solve $9^{19} \bmod 35$

$9^2 \equiv 81 \equiv 11 \bmod 35$

$9^4 \equiv (9^2)^2 \equiv (11)^2 \equiv 121 \equiv 16 \bmod 35$

$9^8 \equiv (9^4)^2 \equiv (16)^2 \equiv 256 \equiv 11 \bmod 35$

$9^{16} \equiv (9^8)^2 \equiv 11^2 \equiv 16 \bmod 35$

$\Rightarrow 9^{19} \equiv 9^{16} \cdot 9^2 \cdot 9 \equiv 16 \cdot 11 \cdot 9 \equiv 1584 \equiv 9 \bmod 35$

$\therefore$ original message : 9

Ex6 (T11 - Q7) Suppose that Eve sees that Bob has provided $k = 11$ and $N = 65$, and Alice set Bob the encoded message $b = 3$. What is the secret message?

How to **decrypt** given b, N, and k.

$\Rightarrow$ Solve $x^k \equiv b \bmod N$
$\Rightarrow$ $x^{11} \equiv 3 \bmod 65$

$\emptyset(65) = \emptyset(13)\,\emptyset(5) = 12\times4 = 48$

① Check $\gcd(k, \emptyset(n)) = \gcd(11, 48) = 1$
$\gcd(b, n) = \gcd(3, 65) = 1$
} We can find a solution!

The solution for $x^{11} \equiv 3 \bmod 65$ is 3^y where y is the solution of $11y \equiv 1 \bmod 48$

② Solve $11y \equiv 1 \bmod 48$

$48 = 11\times4 + 4$
$11 = 4\times2 + 3$
$4 = 3\times1 + 1$

$\rightarrow$
$1 = 4 - 3\times1$
$1 = 4 - (11 - 4\times2)\times1$
$1 = 4 - 11\times1 + 4\times2$
$1 = 4\times3 - 11\times1$

$$1 = (48 - 11\times 4)\times 3 - 11\times 1$$
$$1 = 48\times 3 - 11\times 12 - 11\times 1$$
$$1 = 48\times 3 + 11\times(-13)$$

$\rightarrow y = -13 \equiv 35 \bmod 48$

③ The solution of $x^{11} \equiv 3 \bmod 65$ is $x = 3^{35}$
i.e. Solve $3^{35} \bmod 65$

$3^2 \equiv 9 \bmod 65$

$3^4 \equiv (3^2)^2 \equiv 81 \equiv 16 \bmod 65$

$3^8 \equiv (3^4)^2 \equiv 16^2 \equiv 256 \equiv 61 \equiv -4 \bmod 65$

$3^{16} \equiv (3^8)^2 \equiv (-4)^2 \equiv 16 \bmod 65$

$3^{32} \equiv (3^{16})^2 \equiv 16^2 \equiv 61 \equiv -4 \bmod 65$

$3^{35} \equiv 3^{32}\cdot 3^2 \cdot 3 \equiv (-4)\times 27 \equiv -108 \equiv 22 \bmod 65$

$\therefore$ original message: 22.