# Prime Numbers

A Prime Number can be divided evenly only by 1 or itself and it must be a whole number greater than 1. Some examples:

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 | 53 | 59 | 61 | 67 |
| 71 | 73 | 79 | 83 | 89 | 97 | 101 | 103 | 107 | 109 | 113 | 127 | 131 | 137 | 139 | 149 | 151 | 157 | 163 |
| 167 | 173 | 179 | 181 | 191 | 193 | 197 | 199 | 211 | 223 | 227 | 229 | 233 | 239 | 241 | 251 | 257 | 263 | 269 |
| 271 | 277 | 281 | 283 | 293 | 307 | 311 | 313 | 317 | 331 | 337 | 347 | 349 | 353 | 359 | 367 | 373 | 379 | 383 |
| 389 | 397 | 401 | 409 | 419 | 421 | 431 | 433 | 439 | 443 | 449 | 457 | 461 | 463 | 467 | 479 | 487 | 491 | 499 |
| 503 | 509 | 521 | 523 | 541 | 547 | 557 | 563 | 569 | 571 | 577 | 587 | 593 | 599 | 601 | 607 | 613 | 617 | 619 |
| 631 | 641 | 643 | 647 | 653 | 659 | 661 | 673 | 677 | 683 | 691 | 701 | 709 | 719 | 727 | 733 | 739 | 743 | 751 |
| 757 | 761 | 769 | 773 | 787 | 797 | 809 | 811 | 821 | 823 | 827 | 829 | 839 | 853 | 857 | 859 | 863 | 877 | 881 |
| 883 | 887 | 907 | 911 | 919 | 929 | 937 | 941 | 947 | 953 | 967 | 971 | 977 | 983 | 991 | 997 | | | |

Source: https://www.mathsisfun.com/prime_numbers.html

Online Prime Checker: https://www.calculatorsoup.com/calculators/math/gcf.php

# Greatest Common Divisor (GCD)

The greatest common divisor, sometimes also called the highest common divisor of two positive integers **a** and **b** is the largest divisor common to **a** and **b**. It is also known as the Greatest Common Factor (GCF), or Highest Common Factor (HCF). Greatest Common Divisor (GCD) for 12 18 is 6 expressed as GCD(12,18)=6

More examples: GCD(12,60)=12, and GCD(12,90)=6, GCD(3,5)=1.

Source: http://mathworld.wolfram.com/GreatestCommonDivisor.html

Online Calculator: https://www.calculatorsoup.com/calculators/math/gcf.php

# Co-Prime or Relatively Prime

- In mathematics, two integers (*a* and *b*) are **coprime** (or **relatively prime**) if they share no common factors. In other words, there is no number, other than 1, that divides both *a* and *b* evenly. This is equivalent to their greatest common divisor being 1 i.e. *gcd(a,b)=1*

- An example: 6 and 35 are coprime, because the factors of 6, 2 and 3, do not divide 35 evenly. 6 and 27 are not coprime, because 3 divides both 6 and 27.

Source: https://simple.wikipedia.org/wiki/Coprime
Online co-prime checkers:
https://www.dcode.fr/coprimes
http://www.numere-prime.ro/coprime-numbers-relatively-prime.php

# Modular Arithmetic – MOD

Modular arithmetic involves division of integers with an associated remainder. Given two integers, *m* and *n*, *m* mod *n* is defined as the remainder when m is divided by n. This is commonly written as

$$m \bmod n = r$$

Where *r* is the remainder of *m/n*.. The term *r* is sometimes referred to as the residue.

Examples

*4* mod *3 = 1; 21* mod *5 = 1; 20* mod *4 = 0*

Some useful property.

*(x.y) mod n= (x mod n. y mod n) mod n*

*Example: 400 mod 15= (20.20) mod 15*

*= (20 mod 15 x 20 mod 15) mod 15*

*= (5 x 5) mod 15*

*= 25 mod 15*

*=10*

You can use (i.e. split the numbers) this when the numbers are large.

# Calculating Large MOD

We can split the numbers when the numbers are large. So, the property we learned earlier is useful. But for very large numbers we have to use software program (e.g. java/c/c++ code) or online calculators. Here are some examples:

$$8596^{283} \; mod \; 16999 = 16809$$

**PowerMod Calculator**

Computes (base)$^{(\text{exponent})}$ mod (modulus) in log(exponent) time.

| Base: 8596 | Exponent: 283 | Modulus: 16999 |
|---|---|---|
| Compute | $b^e$ MOD $m$ = | 16809 |

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

$$16809^{7267} \; mod \; 16999 = 8596$$

**PowerMod Calculator**

Computes (base)$^{(\text{exponent})}$ mod (modulus) in log(exponent) time.

| Base: 16809 | Exponent: 7267 | Modulus: 16999 |
|---|---|---|
| Compute | $b^e$ MOD $m$ = | 8596 |

The program is written in JavaScript, and runs on the client computer. Most implementations seem to handle numbers of up to 16 digits correctly.

Online Calculator: https://www.mtholyoke.edu/courses/quenell/s2003/ma139/js/powermod.html

# Calculating Inverse MOD

Say, $d * 7 = 1 \bmod 20$. How do you calculate $d$?

Here, $d$ is the multiplicative inverse of $7$ modulo $20$. This can be solved using Extended Euclid Algorithm.

*Note: It's out of the scope to learn this algorithm during the lecture. We will use intuitive argument for small numbers, and online calculator for large numbers (next slide). Tutors will provide links to online resources.*

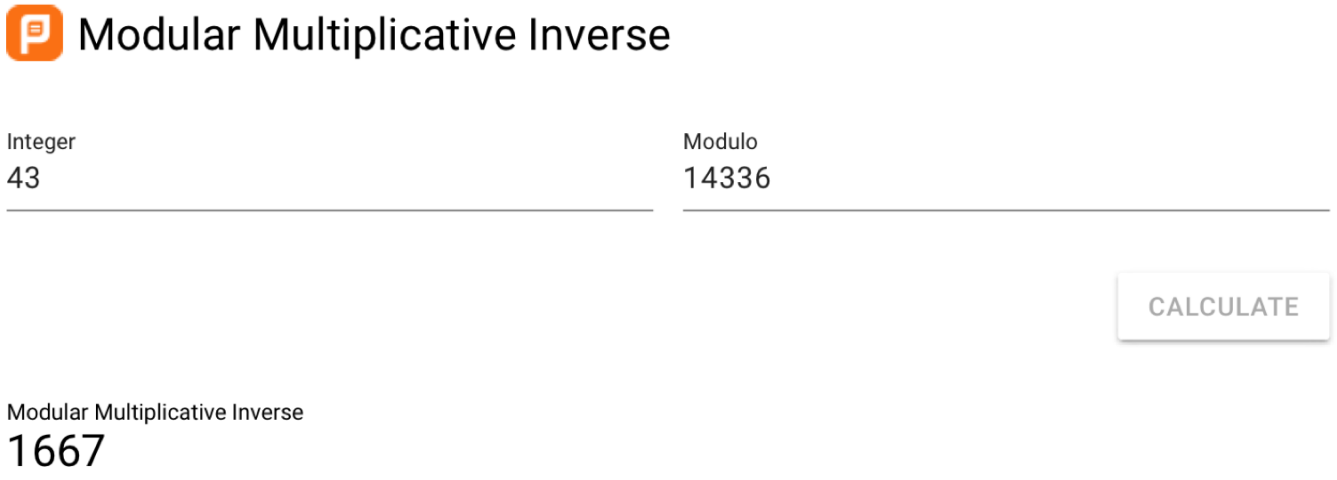
intuitive argument

For simplicity, $d * 7 = 1 \bmod 20$ can be interpreted as follows: ( $d * 7$ ) / 20 = "something" with the remainder of 1. We can easily conclude that 21 / 20 gives "something" with the remainder of 1. So, $d * 7 = 21$, and $d = 3$

# Calculating Large Inverse MOD

We can use software program (e.g. java/c/c++ code) or online calculators when we large numbers. Here are some examples:

$d * 43 = 1 \ mod \ 14336$ What is the value of $d$?




Using Extended Euclid Algorithm $d = 1667$

Online Calculator: https://planetcalc.com/3311/

# Least Common Multiple (LCM)

The Least Common Multiple (LCM) is also referred to as the Lowest Common Multiple (LCM) and Least Common Denominator (LCD). For 2 integers a and b, denoted LCM(a,b), it is the smallest integer that is evenly divisible by both a and b. For example, LCM(2,3) = 6 and LCM(6,10) = 30. LCM(5,15) = 15

Online Calculator: https://www.calculatorsoup.com/calculators/math/lcm.php