Number Theory Cheat Sheet

Number theory is a branch of mathematics that is concerned with the study of the properties of numbers, and the interesting and unexpected relationships between different sorts of numbers. Of course, these relationships also need to be proved true. Number theory is used in cryptography.

The division algorithm

Systems of numbers can be referred to in different ways, it is important to know what each system refers to:

- The integers, $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The natural numbers $\mathbb{N} = \{1, 2, 3, \ldots\}$
- You may have already come across the real numbers, $\mathbb{R}$, or the rational numbers, $\mathbb{Q}$.

It is important to note that the set of natural numbers **does not** contain 0. The union of the set of natural numbers with 0 is denoted $\mathbb{N}_0$.

Divisibility is a very important concept in number theory. Although you will have seen the concept of divisibility before and will be very used to working with it, it is very useful to define it:

- If a and b are integers with $a \neq 0$, then b is divisible by a if there exists an integer k such that $b = ka$. If this happens, then we say that a divides b, which is denoted $a|b$. If a does not divide b then we write $a \nmid b$

This definition considers both positive and negative divisors. Divisibility also has the following properties:

For any $a, b, c \in \mathbb{Z}$, with $a \neq 0$:

- $a|a$ (every integer divides itself)
- $a|0$ (0 is divisible by any integer)
- If $a|b$ and $b|c \Rightarrow a|c$
- If $a|b$ and $a|c \Rightarrow a|bn + cm$ for all $m, n \in \mathbb{Z}$
- $a|b \Leftrightarrow an|bn$ for all $n \in \mathbb{Z}, n \neq 0$
- If a and b are positive integers and $a|b$ then $a \leq b$

Example 1: Prove that If $a|b$ and $b|c \Rightarrow a|c$

Use the fact that a divides b to rewrite b in terms of a and c in terms of b	$b = ka$, for some $k \in \mathbb{Z}$. $c = hb$, for some $h \in \mathbb{Z}$
Substitute the equations into each other	$c = h(ka)$, or $c = (hk)a$ As $h, k \in \mathbb{Z}$, $h \times k \in \mathbb{Z}$, as the set of integers are closed under multiplication, so $a|c$

The set of integers being closed under multiplication means that an integer multiplied by an integer will always give an integer. The same is true for addition and subtraction with the set of integers but is not always true for division.

Because of this, it's helpful to have a better definition for division with the integers- the division algorithm allows us to find a unique quotient and remainder for any two integers:

If a and b are integers such that $b > 0$, then there exists unique integers q (which can be referred to as the quotient) and r (remainder) such that $a = bq + r$, with $0 \leq r < b$. The process to find these integers is called the division algorithm:

1. Begin with your values of a and b
2. Set q equal to the greatest integer that is less than or equal to $\frac{a}{b}$
3. Set $r = a - bq$

Note that a is divisible by b if and only if $r = 0$.

Example 2: Find the quotient and remainder when 4649 is divided by 56

Set the values of a and b.	$a = 4649$ $b = 56$
Find the value of q	$\frac{a}{b} = 83.0178$ $q = 83$
Find the value of r	$r = a - bq$ $r = 4649 - (56)(83)$ $r = 1$ $4649 = 56(83) + 1$

The Euclidean algorithm

Using the previous work on divisibility, we can write formal definitions of common divisors and greatest common divisors:

- For $a, b, c \in \mathbb{Z}$, and $c \neq 0$, c is a common divisor of a and b is $c|a$ and $c|b$
- The greatest common divisor, d, of $a, b \in \mathbb{Z}$, satisfies the following conditions:
  - $d|a$ and $d|b$
  - If c is a common divisor of a and b, then $c \leq d$

The greatest common divisor of a and b can also be denoted gcd (a, b)

As you will have seen before, the greatest common divisors can be found by writing the number as a product of prime factors, but this is an inefficient method for large numbers. The Euclidean algorithm provides an iterative method for finding the greatest common divisor of two integers:

1. Given your two integers, denote them a and b such that $a \geq b$
2. Use the division algorithm to find integers q_1 and r_1 such that $a = q_1 b + r_1$. If $r_1 = 0$, then $b|a$ and $\gcd(a, b) = b$.
3. If $r_1 \neq 0$, apply the division algorithm to b and r_1 to find integers q_2 and r_2 such that $b = q_2 r_1 + r_2$ where $0 \leq r_2 < r_1$. If $r_2 = 0$, then $\gcd(a, b) = r_1$
4. If $r_2 \neq 0$, continue the process. The last non-zero remainder is the greatest common divisor of a and b.

Example 3: Use the Euclidean algorithm to find the greatest common divisor of 765 and 212

Apply the division algorithm to 765 and 212	$\frac{765}{212} = 3.6085$ $q = 3$ $r = 765 - 212(3) = 129$ $765 = 3(212) + 129$
Apply the division algorithm to the original divisor and the remainder	$212 = 1(129) + 83$
Continue applying the division algorithm	$129 = 1(83) + 46$ $83 = 1(46) + 37$ $46 = 1(37) + 9$ $37 = 4(9) + 1$ $9 = 9(1) + 0$
As the last non-zero remainder is 1, that is the gcd.	$\gcd(765, 212) = 1$

The Euclidean algorithm and back-substitution can be used to write the greatest common divisor of two numbers as a linear combination of itself:

- Bezout's identity states that for $a, b \in \mathbb{Z}, \neq 0$, then there exists $x, y \in \mathbb{Z}$ such that $\gcd(a, b) = ax + by$

Example 4: Use the Euclidean algorithm to find $x, y \in \mathbb{Z}$ such that $312x + 403y = \gcd(312, 403)$

Apply the Euclidean algorithm	1- $403 = 312(1) + 91$ 2- $312 = 91(3) + 39$ 3- $91 = 39(2) + 13$ 4- $39 = 13(3) + 0$ $\gcd(312, 403) = 13$
Apply Bezout's theorem	By Bezout's theorem, there exists integers x and y such that $13 = 312x + 403y$
Work backwards through the Euclidean algorithm Rearranging eqn 3 Substituting eqn 2 Substituting eqn 1	$13 = 91 - 39(2)$ $13 = 91 - (312 - 91(3))(2)$ $13 = 91 - 2(312) + 6(91)$ $13 = 7(91) - 2(312)$ $13 = 7(403 - 312) - 2(312)$ $13 = 7(403) - 7(312) - 2(312)$ $13 = 7(403) - 9(312)$

In example 3, the gcd of 765 and 212 was 1. Integers with a gcd of 1 are said to be relatively prime:

- Two integers a and b are relatively prime if $\gcd(a, b) = 1$
- The integers a and b are relatively prime if and only if there exist integers x and y such that $ax + by = 1$

Modular arithmetic

As seen before, when two numbers a and b are divided, they can be written in the form $a = qb + r$, where q is the quotient and r is the remainder. Sometimes, we are only interested in the remainder, and therefore we can use the modulo operator. Modular arithmetic is used daily when looking at analogue clocks. One hour after midnight, the hour hand each points at 1. The hour hand next points at 1 after 12 hours have passed- which is equivalent to 13 hours after midnight. This shows us that $1 \equiv 13$ mod 12, and therefore 13 and 1 are congruent. It is important to note that although 1 and 13 are congruent with respect to modulo 12, they would not be congruent to modulo 5, for example.

- For a positive integer m, the integer a is congruent to the integer b modulo m if $m|(a - b)$
- $a \equiv b(\text{mod } m)$ if and only if a and b leave the same remainder when they are divided by m

Example 5: Is the statement $26 \equiv 8$ mod 3 true?

Apply the rule 'for a positive integer m, the integer a is congruent to the integer b modulo m if $m|(a - b)$'	$26 - 8 = 18$ $18 \div 3 = 6$ So $3|18$ and the statement is true

Adding or subtracting integer multiples of the modulus (in the previous example the modulus was 3) produces congruent numbers:

- For $a, b, m \in \mathbb{Z}$, with $m > 0$ then $a \equiv b(\text{mod } m)$ if and only if there exists $k \in \mathbb{Z}$ such that $a = b + km$

Modula arithmetic also has the following useful properties:

For $a, b, c, d, m, n \in \mathbb{Z}$ and $m, n > 0$

- $a \equiv 0(\text{mod } m)$ if and only if $m|a$
- $a \equiv a(\text{mod } m)$
- If $a \equiv b(\text{mod } m)$, then $b \equiv a(\text{mod } m)$
- If $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$, then $a \equiv c(\text{mod } m)$

If $a \equiv b(\text{mod } m)$ and $c = d(\text{mod } m)$ then:

- $a \pm c \equiv b \pm d(\text{mod } m)$
- $ac \equiv bc(\text{mod } m)$
- $ka \equiv kb(\text{mod } m)$
- $a^n \equiv b^n(\text{mod } m)$

Divisibility tests

You will have some simple rules that you use to know if a number is divisible by 2, 5, or 10. For example a number is divisible by 2 if it is even, divisible by 5 if its end digit is either 0 or 5 and divisible by 10 if and only if it ends in 0. These results can be rigorously proven using modular arithmetic, by writing the numbers as a sum of its digits multiplied by its power of 10, for example as

$$10^n a_n + 10^{n-1} a_{n-1} + 10^{n-1} a_{n-2} + \cdots + 10a_1 + a_0$$

The a_i are called decimal digits.

For example, 67253 would be written as $10^4 \times 6 + 10^3 \times 7 + 10^2 \times 2 + 10 \times 5 + 3$.

Using the simple rules you already know, and some new ones, you can use modular arithmetic to prove divisibility:

- An integer is divisible by 3 if and only if the sum of the digits is divisible by 3
- An integer is divisible by 4 if and only its last two digits are divisible by 4
- An integer is divisible by 6 if and only if it is divisible by 2 and 3
- An integer is divisible by 9 if and only if the sum of its digits is divisible by 9
- An integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11

Example 6: Prove that a three-digit number is divisible by 9 if and only if the sum of its digits is divisible by 9

Write the general form of a three-digit number using the form above	$N = 100(a) + 10(b) + c$ $a, b, c \in \{0,1,2,3,4,5,6,7,8,9\}, a \neq 0$
Use the modulo of 100 and 10 to rewrite the number in terms of the decimal digits	$100 \equiv 1$ mod 9 $10 \equiv 1$ mod 9 For the number to be divisible by 9, it must equal 0 mod 9, therefore by the multiplication rules for modular arithmetic: $N = 0$ mod 9 if and only if $a + b + c = 0$ mod 9

Solving congruence equations

Equations using modular congruences are called congruence equations and can be solved using modular arithmetic. The solutions are usually given in terms of least residues, which is the set $\{0, 1, 2, 3, \ldots, n-2, n-1\}$ for modulo n.

Example 7: Solve the equation $x + 12 \equiv 5$ mod 6

Subtract 12 from both sides	$x \equiv 7$ mod 6
Write as a least residue, negative numbers can be confusing within modular arithmetic, but the process is still the same. $-\frac{7}{6} = -1.166$, and the next lowest integer from this is -2. To get from -2×6 to -7, we must add 5, so our remainder is 5. This can also be shown by repeatedly adding 6 until you get to a number that is in the set of least residues	$x \equiv 5$ mod 6

Equations of the form $ax \equiv b$ mod m are more difficult some may have no solutions, and some can have many:

Let $a, b, m \in \mathbb{Z}$, with $m > 0$ and $\gcd(a, m) = d$

- If $d \nmid b$, then the equation $ax \equiv b$ mod m has no solutions
- If $d|b$ then the equation $ax \equiv b$ mod m has d solutions in the set of least residues modulo m.

If you know that the equation has a solution, and it has been reduced as much as possible by cancelling, then you need to find a multiplicative inverse. The multiplicative inverse of a mod m is in integer p that satisfies $ap \equiv 1$ mod m. The multiplicative inverse exists if and only if $\gcd(a, m) = 1$

Example 8: Find a multiplicative inverse of 7mod 31 and solve the equation $7x \equiv 13$ mod 31

Find the gcd using the Euclidean algorithm	$31 = 4(7) + 3$ $7 = 2(3) + 1$ $3 = 3(1) + 0$ So $\gcd(7, 31) = 1$
Work backwards through the steps in the Euclidean algorithm	$1 = 7 - 2(3)$ $1 = 7 - 2(31 - 4(7))$ $1 = 9(7) - 2(31)$ $9(7) = 1 + 2(31)$ So, 9 is a multiplicative inverse of 7 mod 31
Multiply both sides of the equation by the multiplicative inverse	$7x \equiv 13$ mod 31 $9(7x) \equiv 9 \times 13$ mod 31 $x \equiv 117$ mod 31 $x \equiv 24$ mod 31

If $\gcd(a, m) \neq 1$, then there are two possible methods:

Method 1: Use back substitution to find a linear combination of a and m that equals the gcd. Multiply this linear combination by $\frac{b}{\gcd(a,m)}$ so it is in the form $ka \equiv b(\text{mod } m)$, k will be one solution and add multiples of $\frac{m}{\gcd(a,m)}$ to find gcd (a, m) distinct solutions modulo m	**Method 2:** Divide everything by $\gcd(a, m)$to have an equation of the form $px \equiv q(\text{mod } r)$ with p and r relatively prime Find a multiplicative inverse for p modulo r and multiply through by this inverse

Fermat's little theorem

Fermat's little theorem is used to find least residues of powers easily, and solve congruence relationships involving them quickly:

If p is prime and a is not divisible by p, then:

- $a^{p-1} \equiv 1$ mod p
- $a^p \equiv a$ mod$p$

Combinatorics

Combinatorics deals with counting and the number of combinations- you should already know that if one item can be chosen m different ways and another item can be hosen n different ways then the total combinations is $m \times n$. This can be extended to more than two items and more advanced situations can be modelled by adding/subtracting possibilities.

- If a set S contains n elements, then the total number of possible subsets is 2^n

The product rule can also be used to count the number of ways things can be arranged, called permutations. It is important to note that once an item has been put in place, it isn't counted in the possibilities for another space, so

- There are $n!$ Different ways of placing n items in order
- The number of permutations of r items from a set of n items, where $n \geq r$, is given by ${}^nP_r = \frac{n!}{(n-r)!}$
- The number of permutations of n items, of which r are identical, is given by $\frac{n!}{r!}$
- This can be extended to a situation of n items, of which r_1 are identical, r_2 are identical etc is given by $\frac{n!}{r_1! \times r_2! \times \ldots}$
- The number of possible combinations of r items (in any order) taken from a set of n items, where $n \geq r$ is given by ${}^nC_r = \binom{n}{r} = \frac{n!}{(n-r)!r!}$ – you have encountered this formula before when looking at the binomial theorem.

Example 9: How many 6-digit numbers can be made from the numbers 1, 2, 3 and 4, provided that the number 1 must appear exactly once, and every other number must appear at least once

Notice that two extra digits must be added	We know that the number must feature the digits 1,2,3 and 4. The digits that can be the two 'extra' are {2,2}, {3,3}, {4,4}, {2,3}, {2,4} or {3,4} (the order of these extra digits doesn't matter yet)
Consider the case where the same letters are added	When the same letters are added, we are looking at a permutation of 6 digits, of which 3 are identical, thus the permutation is $\frac{6!}{3!}$
Consider the case where different letters are added	When different letters are added, we are looking at a permutation of 6 digits, of which two sets of two are identical, thus the permutation is $\frac{6!}{2! \times 2!}$
Find the total number of permutations	Each case can happen in 3 different ways, so the total number of permutations is given by $3\left(\frac{6!}{3!}\right) \times 3\left(\frac{6!}{2! \times 2!}\right) = 900$