# Basics of Number Theory

**I have used the divisibility definition several times. Here I will present it again, as we delve more deeply into its uses. We will say that an integer a divides an integer b evenly without a remainder, like this: a | b. This implies that there exists an integer c such that b = ac. We will only define division by non-zero integers. Hence, it is not permissible to write 0 | a.**

**Here are some rules that division of integers follow. (Note, a, b and c are always non-zero integers.)**

**1) 1 | a**
**2) a | 0**
**3) if a | b, and b | c, then a | c.**
**4) if a | b and b | a, then a = +b or a = -b**
**5) if x = y + z, and we have a | y and a | z, then a | x as well.**
**6) if a | b and a | c, then we have a | bx + cy for all ints x and y.**

**Examples of how we can use these rules is as follows:**

**Problem #1**
**Are there any integer solutions to the equation 5x + 10y = 132?**

**The answer is no. We know that 5 must divide 5x and it must also divide 10y, thus 5 | (5x+10y). (Rule 6) We can see this clearly by factoring the expression as 5(x+2y). But we know that 5 | 132 is false, thus, there is no solution. One more way we can see this is by the following:**

**5(x+2y) = 132**
**x+2y = 132/5, since x and y are ints, x+2y is, but 132/5 is not, and since the integers are closed over addition, there are no integer solutions that satisfy the equation.**

**Problem #2**

**If x and y are integers such that 13 | (3x+4y), prove that 13 | (7x+5y). Note that we can rewrite 7x+5y as 13x + 13y – 2(3x+4y). So we have:**

**7x + 5y = 13(x+y) – 2(3x + 4y)**

**Let A = x+y, B=3x+4y**

**We have 7x+5y = 13A – 2B.**

**Since 13 | B, we can express B=13B', where B' is an integer.**

**Thus we have**

**7x+5y = 13A – 2B = 13A – 2(13B') = 13A – 26B' = 13(A – 2B')**
**By definition of divisibility, we have 13 | (7x+5).**

**Notice that we came up with the original expression "out of the blue." One way to do this is trial and error, playing around with different multiples of 13x and 13y and adding or subtracting different multiples of 3x+4y until you obtain 7x+5y. It turns out that there is a systematic way to obtain an appropriate expression and this will be covered in a future lecture.**

# The Division Algorithm

**This is simply a symbolic representation of what you've known since grade school. If you divide one number by another, the remainder is always in between 0 and that number-1. Here it is:**

**If a, b $\in$Z, with b > 0, then there exists unique q, r$\in$Z such that**

**$a = qb + r, 0 \leq r < b$.**

**So, this just says when you divide a by b, you get a quotient of q, with a remainder of r in between 0 and b-1, such that both q and r are integers, and there is exactly one ordered pair (q, r) that satisfies these requirements.**

**First we prove that at least one solution to the given equation with the restrictions on q and r exist.**

**We can prove this by contradiction. Let's assume that no such q and r exist. We know that without the restriction $0 \leq r < b$, we can find q=0 and r=a that will work. If a < b, we have shown there is at least one solution. Thus, we assume a > b.**

**Let's assume that the smallest r$\geq$0 for which a = qb + r is greater than or equal to than b. Let this r = b + r', where r' $\geq$ 0. So, we have:**

**$a = qb + r$**
**$= qb + b + r - b$, now let r'=r – b.**
**$= (q+1)b + r'$**

**Thus, we have found new integers q'= q+1 and r'=r-b such that**
**$a = q'b + r'$, where $0 \leq r' < r$. But, that contradicts our assumption that r was the smallest integer greater than or equal to 0 that satisfied the requirement. Thus, we must have at least one solution of**

**$a = qb + r$ such that $q, r \in Z \wedge 0 \leq r < b$.**

**Now, we must show that there are no other pairs (q,r) that satisfy this equation. Let's use proof by contradiction again.**

**Assume there are two distinct pairs of integers (q,r) and (q',r') such that**

**$a = qb + r = q'b + r'$, with $0 \leq r,r' < b$.**

**Then, we have:**

**$qb - q'b = r' - r$**
**$b(q - q') = r' - r$**

**Either $q - q' \neq 0$ or $r' - r \neq 0$.**

**If $q - q' \neq 0$, then we have $|b(q - q')| \geq b$, but we know that $|r' - r| < b$, since $0 \leq r,r' < b$. Thus, this case is impossible.**

**Otherwise, we must have $r' - r \neq 0$. But, this too is impossible since we have $0 < |r' - r| < b$, and we know that this can NOT be a multiple of b like $b(q - q')$ is.**

**Thus, we have contradicted our assumption that either $q - q' \neq 0$ or $r' - r \neq 0$, proving that q and r are unique.**

## Application of Division Algorithm: Base Conversion

**Our regular counting system is the decimal (base 10) system. This is because we use 10 distinct digits, zero through nine. In general, the numerical value of a number is what you were taught in elementary school. For example,**

$$2713 = 2 \times 10^3 + 7 \times 10^2 + 1 \times 10^1 + 3 \times 10^0$$

**Each digit's value is determined by which place it's in. Each place is a perfect power of the base, with the least significant at the end, counting up by one as you go through the number from right to left.**

**Although this seems to be the only possible number system, it turns out that the number of digits used is arbitrary. We could have just as easily chose to use 5 digits (0 – 4), in which case the value of a number would be as follows:**

**$314_5 = 3 \times 5^2 + 1 \times 5^1 + 4 \times 5^0 = 84_{10}$.**

**Thus, this is how we convert from a different base to base 10. (Note that we write a subscript by the number to denote its base.) In general, we can write our conversion as follows:**

**$d_{n-1}d_{n-2}\ldots d_2d_1d_0$ (in base b) $= d_{n-1}xb^{n-1} + d_{n-2}xb^{n-2} + \ldots + d_2xb^2 + d_1xb + d_0$**

**(Note, b raised to the 1 and 0 powers were simplified above.)**

**Let's look at a couple quick examples:**

**$781_9 = 7x9^2 + 8x9^1 + 1x9^0 = 640_{10}$**

**$1110101_2 = 1x2^6 + 1x2^5 + 1x2^4 + 0x2^3 + 1x2^2 + 0x2^1 + 1x2^0 = 117_{10}$**

**(Note: Base 2 is so common, it has a name: binary.)**

**Now, let's consider the opposite problem: taking a number, X, in base 10 and converting it to base b:**

**Our number's value in base ten can be expressed as:**

**$X = d_{n-1}xb^{n-1} + d_{n-2}xb^{n-2} + \ldots + d_2xb^2 + d_1xb + d_0$**

**$= b(d_{n-1}xb^{n-2} + d_{n-2}xb^{n-3} + \ldots + d_2xb^1 + d_1xb^0) + d_0$**

**We factored out b from all the terms except for the last. We can think of X as the number we are dividing into and b as the number we are dividing by. Viewing this equation in this fashion, then the corresponding quotient and remainder are:**

**Quotient = $(d_{n-1}xb^{n-2} + d_{n-2}xb^{n-3} + \ldots + d_2xb^1 + d_1xb^0)$**
**Remainder = $d_0$**

**What this indicates immediately is that if we want to convert a number from base 10 to another base b, we can reveal the least significant "digit" of the answer via the division algorithm.**

**If we glance more carefully at these two results, we can see that the expression for the quotient is essentially the base 10 value of "the rest of the number" except for the last digit. Thus, if we want to complete our base conversion task, we can just divide this new quotient by b and that will reveal $d_1$. If we repeatedly divide the new quotient from each subsequent division by b, we'll reveal each digit of the number converted to base b, in reverse order.**

**Here are some examples:**

**<u>Problem 3: Base Conversion Example</u>**
**Convert 117 in base 10 to base 2 (binary)**

**117 = 58 x 2 + 1, 1 ($d_0$)**
**58 = 29 x 2 + 0, 0 ($d_1$)**
**29 = 14 x 2 + 1, 1 ($d_2$)**
**14 = 7 x 2 + 0, 0 ($d_3$)**
**7 = 3 x 2 + 1, 1 ($d_4$)**
**3 = 1 x 2 + 1, 1 ($d_5$)**
**1 = 0 x 2 + 1, 1 ($d_6$), since the quotient is 0, we can stop.**

**To get the result, read the remainders in reverse order: $117_{10} = 1110101_2$**

**Here is a more typical way to write this out:**

**2 | 117**
**2 | 58 R 1 (result of first division, q = 58, r = 1)**
**2 | 29 R 0 (result of second division, q = 29, r = 0)**
**2 | 14 R 1**
**2 | 7 R 0**
**2 | 3 R 1**
**2 | 1 R 1**
**0 R 1**

**We still read the remainders in reverse order to get the result.**

**If a base is bigger than 10, we start using the letters, so a = 10, b = 11, etc. The most typical base bigger than 10 used in computer science is base 16, which is also known as hexadecimal.**

**Problem 4: Base Conversion Example**
**Convert 1327 in base 10 to hexadecimal**

**16 | 1327**
**16 | 82 R 15 (F)**
**16 | 5 R 2**
**0 R 5**

**Thus $1327_{10} = 52F_{16}$**

**Problem 5: Base Conversion Example**
**Convert 693 in base 10 to base 5**

**5 | 693**
**5 | 138 R 3**
**5 | 27 R 3**
**5 | 5 R 2**
**5 | 1 R 0**
**0 R 1**

**Thus $693_{10} = 10233_5$**

# mod relation (in mathematics)

**In math, modulo (mod) is used to define a relationship between integers related to divisibility. Specifically, here is the definition of mod, for integers a, b and positive integer n:**

**$a \equiv b \pmod{n}$ iff $n \mid (a-b)$,**

**Equivalently, we can also say that there exists some integer q such that**

**$nq = a - b$, which also means that**
**$a = b + nq$**

**Here are some true mod relations:**

**$7 \equiv 3 \pmod{4}$**
**$7 \equiv 99 \pmod{4}$**
**$13 \equiv -7 \pmod{10}$**

**In particular with the division algorithm, based on the division algorithm, dividing a by b, it's always true that**

**$a \equiv r \pmod{b}$.**

**More generally,**

**For all integers m, $a \equiv (r+bm) \pmod{b}$. Notice that we can take any mod statement and add or subtract any multiple of the mod value from a value on one side without affecting the truth of the statement.**

**Here are a list of rules using mod, where a, b and c are integers and n and k are positive integers:**

**if $a \equiv b \pmod{n} \Leftrightarrow (a+c) \equiv (b+c) \pmod{n}$**
**if $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$**
**if $a \equiv b \pmod{n} \Rightarrow a^k \equiv b^k \pmod{n}$**
**if $a \equiv b \pmod{n} \Rightarrow f(a) \equiv f(b) \pmod{n}$ for any polynomial f(x) with integer coefficients.**

**if $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$**

**if $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$**

**if $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \Rightarrow ac \equiv bd \pmod{n}$**

**These can all be rigorously proved. Let's just take a quick look and prove the following statement which is a specific case of the exponent rule with k = 2:**

**Problem 6: Mod Proof from First Principles**
**Prove the following for all integers a and b, and positive integers n:**

**if $a \equiv b \pmod{n} \Rightarrow a^2 \equiv b^2 \pmod{n}$**

**Proof #1**
**By definition of mod, we must prove that $n \mid (a^2 - b^2)$. We may assume that $n \mid (a - b)$.**

**Therefore, there exists some integer c such that $a - b = cn$.**

**$a^2 - b^2 = (a - b)(a + b) = n(c(a + b))$, since c, a and b are integers, it follows that $c(a + b)$ is as well. Thus, we've proved that $n \mid (a^2 - b^2)$ as desired.**

**Proof #2**
**We may assume that $n \mid (a - b)$. Therefore, there exists some integer c such that $a - b = cn$. Solving for a we get $a = b + cn$. We still aim to prove that $n \mid (a^2 - b^2)$.**

**$a^2 - b^2 = (b + cn)^2 - b^2 = b^2 + 2bcn + c^2n^2 - b^2 = n(2bc + c^2n)$**

**Since b, c and n are all integers, it follows that $2bc + c^2n$ is an integer as well. Thus, we've proven that $n \mid (a^2 - b^2)$**

**It's important to see that these can be proved from first principles. Mostly, moving forward though, we'll use all of these rules to help us solve problems.**

## Mod Proofs

**We can use mod to prove some interesting results. Here are two examples:**

### Problem 7: Squares of Odd Integers

**If n is an odd integer, prove that $n^2 \equiv 1 \pmod 8$.**

**In order to prove this statement, it helps to prove a little lemma:**

**If n is an integer, then n(n+1) is an even integer. We can prove this as follows:**

**n must be even or odd. Let's prove that the given expression is even in both cases. If n is even, there exists an integer c such that n = 2c. Then,**

**n(n+1) = 2c(2c + 1), since c is an integer so is c(2c+1). It follows that n(n+1) is even since we have rewritten it as 2 times an integer.**

**If n is odd, there exists an integer c such that n = 2c + 1. Then,**

**n(n+1) = (2c + 1)(2c + 1 + 1) = 2(2c+1)(c+1), since c is an integer, (2c+1)(c+1) is also an integer, and n(n+1) is also even in this case.**

**Now to prove the given assertion. Since n is odd, there exists an integer a such that n = 2a + 1.**

$$n^2 = (2a + 1)^2 = 4a^2 + 4a + 1 = 4a(a+1) + 1 \equiv 4(2c) + 1 \equiv 8c + 1 \equiv 1 \pmod 8$$

### Problem 8: Squares mod 3

**Prove the following: For all integers a, if $a \equiv 2 \pmod 3$, then $a^2 \equiv 1 \pmod 3$.**

**By definition of mod, there exists an integer c such that a = 3c + 2. Thus.**

**$a^2 = (3c + 2)^2 = 9c^2 + 12c + 4 \equiv 0 + 0 + 4 \equiv 1 \pmod 3$. The key here is that each of the first two terms has a factor of 3, so these reduce to 0 (mod 3).**

# Application of mod: Fast Modular Exponentiation

**It turns out that computing the remainder when a large integer is raised to another large integer and divided by a third large integer is extremely useful in public key cryptography. (Both RSA and El Gamal use this calculation, among other public key schemes.)**

**We can solve these computations quickly either by hand (for smaller cases) or computer (larger cases) by using an algorithm called fast modular exponentiation. In code, usually a top down approach is used, but for computing by hand, a bottom-up approach is typically easier. Only the latter is included in these notes for computation by hand. In general, there are many quick ways by hand to calculate small modular exponents. As long as you understand the mod rules, you can use an "ad hoc" system which just makes sure that you adhere to the mod rules, but does different calculations at different junctures without any necessary pattern per se. Some students prefer a "system", which would be necessary in a computer program, where the same steps are always executed, following struct rules.**

## Fast Modular Exponentiation: Bottom Up Algorithm

**Notice that using the mod rules, if we know that $a^k \equiv b \pmod{n}$, then we can fairly quickly calculate that $a^{2k} \equiv (a^k)(a^k) \equiv b \times b \equiv b^2 \pmod{n}$. We can specifically make sure that the value of b we use in the calculation is such that $|b| < n$. (So sometimes we can use the positive value, other times the negative value, depending on what is closer to 0.)**

**Thus, in a single step, we can double our exponent. This means that for any base, a, and mod value, n, we can calculate the remainders when $a^1$, $a^2$, $a^4$, $a^8$, $a^{16}$, etc. are divided by n in succession.**

**Then, we can use these results to build an answer for a raised to any exponent because every exponent can be represented as a sum of powers of two (binary representation), and then we can just multiply the appropriate terms.**

**This is easiest to see with an example.**

**Problem 9: Fast Modular Exponentiation Calculation**
**What is the remainder when $2^{25}$ is divided by 33?**

**First, let's build our chart of remainders up to $2^{16}$:**

| Exp | 1 | 2 | 4 | 8 | 16 |
|---|---|---|---|---|---|
| $2^{exp}$ %33 | 2 | 4 | 16 | 25 | 31 |

**$2^8 = 16 \times 16 = 256 \equiv 25 \pmod{33}$**
**$2^{16} \equiv 2^8 \times 2^8 \equiv 25 \times 25 \equiv (-8)\times(-8) \equiv 64 \equiv 31 \pmod{33}$**

**The explanation for the last two entries is above.**

**Now, we must express $2^{25}$ as a product of the terms above. Let's convert the exponent 25 to binary:**

**2 | 25**
**2 | 12 R 1**
**2 | 6 R 0**
**2 | 3 R 0**
**2 | 1 R 1**
**0 R 1, thus $25_{10} = 11001$, which means that $16 + 8 + 1 = 25$**

**$2^{25} \equiv 2^{16}2^8 2^1 \equiv (31)(25)(2) \equiv (-2)(-8)(2) \equiv 32 \pmod{33}$.**

**It follows that the remainder when $2^{25}$ is divided by 33 is 32.**

**Problem 10: Modular Exponentiation Simple Base Simplification**
**What is the remainder when $97^{123}$ is divided by 32?**

**Note that $97 \equiv 1 \pmod{32}$. It follows that:**

**$97^{123} \equiv 1^{123} \equiv 1 \pmod{32}$**

**It always makes sense to do the base simplification first before using the actual fast modular exponentiation algorithm. In a special case like this one, it's not necessary, since we know what 1 raised to any power is.**

**Modular Exponentiation – Cycle Method**

**Since there are only so many possible remainders when dividing by n, we are guaranteed that the modular exponentiation calculation "cycles". In particular, if $a^k \equiv 1 \pmod{n}$, particularly for small k, then we can calculate some results to very high exponents very quickly, since we know that the modular exponentiation chart will repeat over and over again. (Similar to if I asked the problem: Melina writes the numbers 1, 6, 3, 7, 2 over and over again. What will be the 2023rd number that she writes? Since she repeats every 5 numbers, we know that the 2021st number will be 1 (since the first 2020 numbers will be the cycle above repeated 404 times), the 2022nd number will be 6 and the 2023rd number will be 3.)**

**Here, the algorithm is to calculate the remainders when $a^0$, $a^1$, $a^2$, $a^3$, $a^4$, … are divided by n until we hit the remainder of 1 again (this was the very first remainder). Then the chart can be used to calculate the remainder when a is raised to any power.**

**Problem 11: Modular Exponentiation Cycle Method**

**What's the remainder when $74^{2023}$ is divided by 11?**

$$74^{2023} \equiv (-3)^{2023} \ (mod\ 11)$$

| Exp | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $(-3)^{exp}$ | 1 | -3 | 9 | 6 | 4 | -1 | 3 | 2 | -6 | 7 | 1 |

**To calculate each subsequent entry in the chart, multiply each previous entry by -3 and reduce the answer mod 11. Here are a few of the calculations in detail:**

**$3^3 = 3^2 \times (-3) = 9 \times (-3) \equiv -27 \equiv 6 \pmod{11}$**

**$3^4 = 3^3 \times 3 = 6 \times (-3) \equiv -18 \equiv 4 \pmod{11}$**

**$3^5 = 3^3 \times 3 = 4 \times (-3) \equiv -12 \equiv -1 \pmod{11}$**

**Since $3^{10} \equiv 1 \pmod{11}$, then $3^{10c} \equiv 1 \pmod{11}$, for any integer c.**

$$74^{2023} \equiv (-3)^{2023} \equiv (-3)^{10\times 202}(-3)^3 \equiv 1^{202}(6) \equiv 6$$

**It follows that the remainder when $74^{2023}$ is divided by 11 is 6.**