Number Theory

Jay Zhao
March 3rd

With two integer d and n we say that d is a divisor of n if there exists some integer a such that $n = da$. We can also say that d "divides" n. Which we write using the following notation:

$$d \mid n$$

Where the middle bar is pronounced "divides"

We have that if $d \mid n$ then $d \mid m \iff d \mid n+m$ a corollary of this is that if $d \mid n$ then $d \nmid m \iff d \nmid n+m$. So for example 9 is a multiple of 3 and 4 is not a multiple of 3. So $9+4=13$ is not a multiple of 3. And 91 is a multiple of 7 and 7 is a multiple of 7. So 98 is also a multiple of 7.

We also have that $d \mid n$ implies that $d \mid an$ for any integer a.

We also also have that if $d \mid n$ and n is not 0 then $|n| \geq |d|$. Since $n = ad$ where a is some integer other than 0, this means that $a \geq 1$ or $a \leq 1$ and thus $|a| \geq 1$. This fact is sometimes used in number theory problems.

Also note that if $d \mid nm$ and $d \nmid n$ then it must be the case that $d \mid n$

Example 1. Prove that if a and b are integers then $7 \mid 10a+b$ if and only if $7 \mid a-2b$ is divisible by 7

Since this is an if and only if problem we have to prove that

$$7 \mid 10a+b \implies 7 \mid a-2b$$

and also that

$$7 \mid a-2b \implies 7 \mid 10a=b$$

I will only prove one direction and leave proving the other direction as an exercise.

$$7 \mid 10a+b \implies 7 \mid 50a+5b \implies 7 \mid 49a+7b+a-2b \implies 7 \mid a-2b$$

Now we define the following equivalence relationship. a and b are equivalent "mod" m if and only if $m \mid a-b$

$$a \equiv b \mod m \iff m \mid a-b$$

We use the $\equiv$ sign because a and b are not literally equal in value, just that they are "equivalent" under our definition.

What this "equivalence" means is that if $a \equiv b \mod m$. For all integers c

$$a+c \equiv b+c \mod m \quad \text{and} \quad ac \equiv bc \mod m$$

It means that if x and y are equivalent then if we replace x by y in any arithmetic expression then the two results are also "equivalent".

So for example if we wanted to find the last digit of the 387^{34} we simply have to notice that the if two numbers have the same last digit then they are equivalent $\mod 10$ because if two number have the same last digit they can only differ in digits past the tens digit, and so the difference must be a multiple of 10, so under $\mod 10$ we can say that

$$387^{34} \equiv 7^{34} \equiv 7^{32} \cdot 7^2 \equiv 2401^8 \cdot 7^2 \equiv 1^8 \cdot 49 \equiv 1 \cdot 9 \equiv 9$$

So the since the two numbers 387^{34} and 9 are equivalent mod 10 then their last digits are also the same.

We can also use this to derive a divisibility test for multiples of 9. Notice that

$$10\ldots00 \equiv 9\ldots99 + 1 \equiv 9 \cdot 1\ldots11 + 1 \equiv 9a + 1 \equiv 1$$

A number $n = a + 10b + 100c + \ldots$ is divisible by 9 if and only

$$9 \mid n \iff 9 \mid n - 0 \iff n \equiv 0 \mod 9$$

We then know that each of 10, 100, 1000, $\ldots$ are $1 \mid 9$. This means that $n \equiv a + b + c + \ldots \mod 9$. And so n is divisible by 9 if and only if the sum of it's digits is also divisible by 9

The only caveat is that we can only replaced x with y when $x \equiv y$ in expressions using only $+$, $-$ and $\times$. So for example while we can do $2^4 \equiv 9^4 \mod 7$ we cannot do $2^4 \equiv 2^{11} \mod 7$ unless we have a really good justification for why we can do it. We cannot do division. If we had $a + c \equiv b + c$ then we can say $a \equiv b$ However if we had $ca \equiv cb$ we cannot then say that $a \equiv b$ as we are dividing both sides by c unless we had really good justification for why we actually can do it.

For example $2 \cdot 1 \equiv 2 \cdot 2 \mod 2$ but $1 \not\equiv 2 \mod 4$.

Example 2. Find all solutions to $x^2 + y^2 = 2025$ where x and y are positive integers. Consider looking at this equation mod 3. That means that

$$x^2 + y^2 \equiv 0 \mod 3$$

since 2025 is divisible by 3

x is either equivalent to 0, 1 or 2 and this gives us that $x \equiv 0$, 1 and 1 respectively. Similarly y^2 is equivalent to either 0 or 1.

Since $x^2 + y^2 \equiv 0 \mod 3$ we must have that both x and y are equivalent to $0 \mod 3$. There exists $x_1 = \frac{x}{3}$ and $y_1 = \frac{y}{3}$ for which

$$9x_1^2 + 9y_1^2 = 2025$$
$$x_1^2 + y_1^2 = 225$$

Again $225 \equiv 0 \mod 3$ so using the same logic as before, x_1 and y_1 are both multiple of 3 Now if we have $x_2 = \frac{x_1}{3}$ and $y_2 = \frac{x_1}{3}$ then we know that

$$x_2^2 + y_2^2 = 5^2$$

for which we can manually verify the only solutions are $(x_2, y_2) = (3, 4), (4, 3)$. We know also that $x = 3x_1 = 9x_2$ and $y = 3y_1 = 9y_2$. Hence $(x, y) = (27, 36), (36, 27)$

Taking mod 3 and mod 4 tends to be useful when dealing with squares because $x^2 = \{0,1\} \mod 3$ and $x^2 = \{0,1\} \mod 4$

Now we will do one last example problem

Example 3. Find **all** positive integers x and y such that

$$3^x - 2^y = 1$$

First we notice that $(x,y) = (1,1)$ is clearly a solution. So we only deal with the case when $y \neq 1$ or in other words when $y \geq 2$

This means that $4 \mid 2^y$, then taking mod 4 we know that

$$3^x \equiv 1 \mod 4$$

if x is odd then $x = 2k+1$ and so

$$3^x \equiv 3^{2k+1} \equiv 9^k \cdot 3 \equiv 1^k \cdot 3 \equiv 3 \not\equiv 1 \mod 4$$

So x cannot be odd and instead x must be even.

So lets write $x = 2k$

$$3^{2k} - 2^y = 1$$

which means that

$$3^{2k} - 1 = 2^y$$

We can now use difference of squares to obtain that:

$$(3^k - 1)(3^k + 1) = 2^y$$

Notice that 2^y has no divisors besides other powers of 2. Or in other words it has no prime divisor other that 2. This means that it must be the case that $3^k - 1$ and $3^k + 1$ have no prime divisors other that 2 and must themselves be powers of 2.

We cannot have that both $3^k - 1$ and $3^k + 1$ are divisible by 4 as that would imply that $4 \mid 3^k + 1 - (3^k - 1)$ and $4 \mid 2$ which is absurd.

So one of $3^k - 1$ and $3^k + 1$ is 2 as $3^k - 1$ and $3^k + 1$ are both even and 2 is the only even power of 2 which is not divisible by 4.

This means that either $3^k + 1 = 2$ which can't be true as $3^k + 1 \geq 3 + 1$

Or we have that $3^k - 1 = 2$ which means $3^k = 3$ and thus $k = 1$. This means that $x = 2$ then

$$3^2 - 2^y = 1$$

and thus

$$2^y = 9 - 1 = 8$$

and then $y = 3$. Which gives us the solution $(x,y) = (2,3)$. We have also proved that these are **all** the solutions.