1 Introduction

Number theory is the study of whole numbers. It is a large field of math that covers many topics and gets quite difficult at higher levels. Here, we will explore some number theory fundamentals known as modular arithmetic. Keep in mind that this handout is written for those who have never seen it before.

1.1 A Loose Definition

Sometimes we would like to know if certain whole numbers are divisible by others, and if not, what remainder they leave upon division. Of course, we could manually divide to find the quotient and remainder, but that's slow and difficult to apply to anything that's not a number. Modular arithmetic helps with that.

We can define some new notation. For integers a, b, n we say that

$$a \equiv b \pmod{n}$$

if and only if a and b leave the same remainder when divided by n. This reads as "a is congruent to b mod n." The congruence $a \equiv b \pmod{n}$ also means that we can write $a = kn + b$ for an integer k or $b = mn + a$ for an integer m; in other words, a and b differ from each other by a multiple of n, which makes sense intuitively because division is just repeated subtraction.

1.2 Basic Results

We begin to play with our new definition.

$$8 \equiv 3 \pmod{5}$$

$$15 \equiv 10 \equiv 0 \pmod{5}$$

$$9 \equiv 15 \pmod{6}$$

$$1001 \equiv 1337 \equiv 11 \equiv 1 \pmod{2}$$

$$-7 \equiv 2 \pmod{9}$$

Immediately we see that congruence is commutative and transitive. We then see that $a \equiv 0 \pmod{n}$ means that a is divisible by n. The next thing to notice is that, for any given n, all integers are congruent exactly one of the numbers $0, 1, 2, \ldots, n-1$ modulo n. It seems like this is always the case because division produces a remainder less than the divisor. We've put a filter over the integers and segregated them by remainder.

The congruence symbol resembles an equals sign. Do they function in the same way? Clearly not. The two numbers on either side of the equivalence aren't necessarily the same number. In fact, in the world modulo n, any numbers that differ by a multiple of n are congruent. However, we see that some basic operations, such as addition and multiplication, still have meaning.

If $a \equiv b \pmod{n}$ and c is an integer,

$$a + c \equiv b + c \pmod{n}$$

$$ac \equiv bc \pmod{n}$$

Which quickly become clear upon the substition $a = kn + b$. Basically, we can add to both sides and multiply to both sides just like we can with equality expressions. Notice how congruence of a and b implies that we can replace a with b in expressions involving addition and multiplication.

From here, we can make more shortcuts. Let $c \equiv d \pmod{n}$. By simply repeatedly applying the above results we have

$$ac \equiv bd \pmod{n}$$

$$a + c \equiv b + d \pmod{n}$$

$$a^k \equiv a \cdot a \ldots a \equiv b \cdot b \ldots b \equiv b^k \pmod{n}$$

Raising both sides of a congruence to a power is especially convenient.

A natural question to ask is if we can derive similar results for division of both sides. Unfortunately, it does not work in reverse: $ac \equiv bc \pmod{n}$ does NOT imply $a \equiv b \pmod{n}$; there is no such cancelation rule. Only under certain conditions does it apply.

Nonetheless, with intuition and some hand-wavy justifications we've elucidated some ideas that might have been obscure without this new tool. Let's see it at work.

1.3 Examples

Example 1 Find the remainder when 7^{2017} is divided by 6.

Solution Note that $7 \equiv 1 \pmod{6}$, so we may rewrite the expression as

$$\begin{aligned} 7^{2017} &\equiv 1^{2017} \pmod{6} \\ &\equiv 1 \pmod{6} \end{aligned}$$

Thus, the remainder is 1. Alternatively, we might have expanded $(6 + 1)^{2017}$ and removed all the terms with factors of 6 to get the same answer. This is essentially the same idea behind modular arithmetic - the derivation of our properties involves substitution, expansion, and removal of unnecessary terms. However, modular arithmetic makes the process extremely quick, and it generalizes a result when an expansion is difficult or impossible.

Example 2 Compute the last two digits of 2017^{50}.

Solution Observe that the last two digits of a number are its remainder when divided by 100.

$$\begin{aligned}
2017^{50} &\equiv 17^{50} \pmod{100} \\
&\equiv (17^2)^{25} \pmod{100} \\
&\equiv (89)^{25} \pmod{100} \\
&\equiv (-11)^{25} \pmod{100} \\
&\equiv (21)^{12} \cdot (-11) \pmod{100} \\
&\equiv (41)^{6} \cdot (-11) \pmod{100} \\
&\equiv (81)^{3} \cdot (-11) \pmod{100} \\
&\equiv 41 \cdot (-11) \pmod{100} \\
&\equiv -51 \pmod{100} \\
&\equiv 49 \pmod{100}
\end{aligned}$$

And we conclude. Each step was simple, and with experience this process (known affectionately as a "mod bash") becomes quick and a matter of computations.

2 Thinking Harder

2.1 Imposing Conditions

Modular arithmetic allows us to quickly check certain conditions that give us extra information. Consider a perfect square n^2. We know that n must be $0, 1, 2, 3 \pmod 4$. Squaring each of these residues and reducing, we see that n^2 is either congruent to $0 \pmod 4$ or $1 \pmod 4$.

Example 3 Find all pairs of integers p, q such that $p^2 + q^2 = 201520152015$.

Solution Using our new insight, we see that the right side is congruent to $3 \pmod 4$ and the left side is the sum of two squares, each either 0 or $1 \pmod 4$. However, it quickly becomes clear that it's impossible for $p^2 + q^2$ to be congruent to $3 \pmod 4$. Thus, there are no solutions.

You might ask, "Why did we have to take the expression mod 4? Why not mod 5?" Yes, you could have taken it mod 5. The right side is $0 \pmod 5$, and we would see that $p \equiv q \equiv 0 \pmod 5$ satisfies our condition. "Aha! We're done, we've found something that works, right?" you might say. However, keep in mind that our mods have only shown is that IF valid p and q exist, it is implied that $p^2 + q^2 \equiv 0 \pmod 5$. We cannot simply say that, because the congruence is satisfied, p and q must exist - one implies the other, but not the other way around. All we're doing is searching for a contradiction or some extra conditions that must be satisfied. In this specific case, mod 5 might give us some conditions to work with, but mod 4 finishes the problem quickly with a contradiction.

Now you might ask, "If some mods work but others don't, how do I know which mod to pick?" Choosing a mod to work in is a skill. It takes experience and intuition. Some general patterns are: squares mod 3, mod 4, or mod 8; cubes mod 9, mod 3, or mod 7; fourths mod 5 or mod 9; etc. Simply writing out the few possibilities and manually computing remainders can give us good information to work with. It's a good idea to take expressions mod some prime if you don't know where to start. Of course, there's always the possibility that mods won't help at all.

2.2 Fermat's Little Theorem and Euler's Totient Function

Up until now, we've simply played around with our definitions and basic properties. Fermat's Little Theorem (he had multiple theorems named for him) presents something a little more nontrivial. It states that for any integer a and prime p,

$$a^p \equiv a \pmod{p}$$

If a is not a multiple of p, then it simplifies to

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

The proof will be omitted here because it is beyond the scope of this introductory handout, but there is a nice combinatorial proof that you may search for online.

This lets us reduce powers much more quickly than before and it opens up proofs for more complex number theoretical ideas. Amazingly, this theorem can be extended beyond primes, with Euler's totient function $\phi(n)$. If n has a prime factorization $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \dots p_k^{\alpha k}$, then $\phi(n) = n(1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$. If a and n are relatively prime integers, then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Notice that in the case that n is prime, $\phi(n) = p - 1$ and we get our friend Fermat's Little Theorem again. Let's revisit an old problem.

Example 4 Find the last two digits of 2017^{50}.

Solution We will take the expression modulo 100 again, but this time we have new knowledge. Note that $\phi(100) = 40$, so we already know that $a^{40} \equiv 1 \pmod{100}$.

$$\begin{aligned}
2017^{50} &\equiv 17^{50} \pmod{100} \\
&\equiv 17^{40} \cdot 17^{10} \pmod{100} \\
&\equiv 17^{10} \pmod{100} \\
&\equiv 89^5 \pmod{100} \\
&\equiv (21)^2 \cdot (89) \pmod{100} \\
&\equiv 41 \cdot (-11) \pmod{100} \\
&\equiv -51 \pmod{100} \\
&\equiv 49 \pmod{100}
\end{aligned}$$

We did less computation by eliminating 17^{40} right from the beginning. This adds a powerful tool to our mod bashing! Higher powers can be reduced much more quickly. However, we will see that this isn't all it's good for.

Example 5 Find all pairs of primes p, q such that $p^3 + q^3 = 4pq + p + q + 12$.

Solution This expression is just begging to be taken mod 3. Doing so, we get

$$p^3 + q^3 \equiv pq + p + q \pmod 3$$

However, we see that, by Fermat's Little Theorem, we can quickly reduce $p^3 \equiv p \pmod 3$ and likewise for q. They cancel from both sides and we are left with

$$pq \equiv 0 \pmod 3$$

p and q are primes, so one of them must be 3. From there, we can substitute into the original expression and solve for the other. We find that the only solution is $(3, 3)$.

2.3 More?

There are many things beyond the scope of this handout. You might search for the Chinese Remainder Theorem, or Wilson's Theorem, or Zsigmondy's Theorem, to name a few, all of which may be expressed using modular arithmetic notation. Much of number theory is beyond the writer of this handout. Keep in mind that number theory is not limited to modular arithmetic.

In conclusion, modular arithmetic facilitates a variety of number theoretical manipulations, making things quick and sleek by writing things in terms of remainders. It has become a tool that number theorists must be familiar with.

3 Problems

A few of these problems require modular arithmetic, but some of them don't. However, they are all number theory problems, so integers are your friends here. You may look for patterns or do some algebra. Later problems get difficult.

1. (AIME) Find the sum of all positive two-digit integers that are divisible by each of their digits.
2. (AMC 10) What is the remainder when $3^0 + 3^1 + 3^2 + \cdots + 3^{2009}$ is divided by 8?
3. (AMC 12) Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?
4. (AMC 10) Leap Day, February 29, 2004, occurred on a Sunday. On what day of the week will Leap Day, February 29, 2020, occur?
5. (AMC 12) Oscar buys 13 pencils and 3 erasers for 1.00. A pencil costs more than an eraser, and both items cost a whole number of cents. What is the total cost, in cents, of one pencil and one eraser?
6. (AIME) Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{999\ 9\text{'s}}$ is divided by 1000.
7. What is the remainder when $2^{123456789}$ is divided by 7?
8. Find all primes p, q such that $p + q = (p - q)^3$.
9. Let $p_1 < p_2 < \cdots < p_{31}$ be primes such that $p_1^4 + p_2^4 + \cdots + p_{31}^4 \equiv 0 \pmod{30}$. Find p_1, p_2, p_3.
10. Show that there exists a prime number between n and $n!$, inclusive for all integers $n > 1$.
11. Find all positive integers n such that $2^4 + 2^7 + 2^n$ is a perfect square.
12. Find the least positive integer n such that n^3 ends in $\ldots 888$.
13. Show that $\binom{p}{k}$ is divisible by p, where p is a prime and $1 \leq k \leq p - 1$.
14. Find all primes p such that $11^{(p^2)} + 1 \equiv 0 \pmod{p}$.
15. Prove that for integers a, b, if $a^5 + 2b^5$ is divisible by 11, then a and b are both divisible by 11.
16. Prove that if a prime $p \equiv 3 \pmod{4}$, then $a^2 + b^2 \equiv 0 \pmod{p}$ implies a and b are both divisible by p.
17. (Wilson's Theorem) Prove that p is a prime if and only if $(p - 1)! + 1 \equiv 0 \pmod{p}$.
18. (IMO) Let a sequence of integers a_n be defined as $a_n = 2^n + 3^n + 6^n - 1$ for $n \geq 1$. Find all positive integers m such that m and a_n are relatively prime for all $n \geq 1$.