Modular Arithmetic

Dennis Chen

NQU

This unit can be described in three words: Take mod something.

1 Divisibility, GCD, and LCM

1.1 Divisibility

Divisibility seems like such a simple idea; if a divides b (which is denoted as $a \mid b$) then $\frac{b}{a}$ must be an integer. However, this falls apart once we start introducing 0 into the equation. For the purpose of letting our definition stay consistent when 0 is introduced, we say that integers $a \mid b$ if there exists integer c such that $ac = b$. (We specify a, b as integer for our useful results to stay consistent.)

This means that all $a \mid 0$ and $0 \nmid b$ for all $b \neq 0$, implying $0 \mid 0$. (Verify this for yourself.)

1.2 Results

Our definition of divisibility leaves us with some helpful results.

Divisibility Results.

1. If $a \mid b$ and $b \mid c$ then $a \mid c$. (This may be referred to as the "chain rule" of divisibility.)
2. If $a \mid b$ then $a \mid bc$ for all integers c.
3. If $a \mid b$ and $a \mid c$, then $a \mid b + c$ and $a \mid b - c$.

2 Modular Arithmetic

The following section describes operations in Modular Arithmetic, intuitively motivated by operations over the integers, rationals, and even real and complex numbers[1]. You will find you will be able to do almost everything $\pmod{n}$ that you would be able to do normally. Make sure you understand the rigorous reasons why these things are true, but you should simultaneously feel free to do whatever you want given a few restrictions.

Modular Congruence. We say $a \equiv b \pmod{n}$ if and only if $n \mid a - b$.

The intuitive way to think about this is that a and b have the same remainder when divided by n. (Remember that negative numbers also have a remainder when divided.)

[1] Yes, you can find $i \pmod{p}$.

Modular Residue. We say the *residue* of an integer $a \pmod{n}$ is the integer b that satisfies

- $0 \leq b < n$
- $a \equiv b \pmod{n}$.

It can be helpful to think of b as the remainder of a when divided by n.

2.1 Modular Operations

You can add, subtract, multiply, and exponentiate modulos. You can also divide, but care must be taken.

Adding. If $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$, $a + b \equiv x + y \pmod{n}$.

Proof. Since $n \mid x - a$ and $n \mid y - b$, clearly $n \mid (x + y) - (a + b)$.

Subtracting is identical, so we do not discuss it further.

Multiplying. If $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$, $ab \equiv xy \pmod{n}$.

Proof. Say $a = a_p n + q$ and $x = x_p n + q$ where q is the residue of a and x, and $b = b_p n + r$ and $y = y_p n + r$ where r is the residue of b and y. Then

$$\begin{aligned} xy - ab &= (x_p n + q)(y_p n + r) - (a_p n + q)(b_p n + r) \\ &= n^2(x_p y_p - a_p b_p) + n(x_p r + y_p q - a_p r - b_p q) + qr - qr \\ &= n^2(x_p y_p - a_p b_p) + n(x_p r + y_p q - a_p r - b_p q), \end{aligned}$$

which is clearly divisible by n.

Exponentiating. For integer a, b and positive integers n, k, if $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$.

Proof. Note that $n \mid a - b \mid a^k - b^k$.

As an exercise for the operations we've defined so far, pick your favorite ordered triple of positive integers (a, b, n), and compute the remainder of $a + b$, $a - b$, ab, and a^b[2] when divided by n.

Dividing. Let a, b, c be positive integers such that $c \mid a$ and $c \mid b$. If $a \equiv b \pmod{n}$ **and** $\gcd(c, n) = 1$, then $\frac{a}{c} \equiv \frac{b}{c} \pmod{n}$.

Be careful to remember that we **must have** $\gcd(c, n) = 1$!
We present the proofs of the divisibility rules as examples.

Example (9 Divisibility Rule). If $n = \overline{d_k d_{k-1} \ldots d_1 d_0}$, prove that $n \equiv d_0 + d_1 + \cdots + d_k \pmod{9}$.

[2] For large enough b, you'll want to know Fermat's Little Theorem!

Solution. Note that $n \equiv 10^0 d_0 + 10^1 d_1 + \cdots + 10^k d_k \equiv d_0 + d_1 + \cdots + d_k \pmod 9$. This works because $10^k \equiv 1^k \equiv 1 \pmod 9$.

Example (11 Divisibility Rule). If $n = \overline{d_k d_{k-1} \ldots d_1 d_0}$, prove that $n \equiv d_0 - d_1 + \cdots + d_k(-1)^k \pmod{11}$.

Solution. Note that $n \equiv 10^0 d_0 + 10^1 d_1 + \cdots + 10^k d_k \equiv d_0 - d_1 + \cdots + d_k(-1)^k \pmod{11}$. This works because $10^k \equiv (-1)^k \pmod{11}$.

Example (AMC 10B 2017/23, nerfed). The positive integer $N = 1234\cdots44$ is the concatenation of the numbers $1, 2, 3, \ldots, 44$. Find the remainder when N is divided by 9.

Solution. It seems somewhat tedious to count the number of occurrences of each digit, which motivates the observation that $4 + 4 \equiv 44 \pmod 9$, and so on for all the two digit numbers. Therefore,

$$N \equiv 1 + 2 + 3 + \cdots + 44 \equiv \frac{44 \cdot 45}{2} \equiv 0 \pmod 9,$$

so the remainder is 0.

Notice that in general, $\overline{ab} \equiv 10a + b \equiv a + b \pmod 9$.

2.2 Modular Inverses

In normal arithmetic, we define $a \cdot a^{-1} = 1$. We can do something similar in modular arithmetic.

Modular Inverse. We define a^{-1} to be the number mod n such that $a \cdot a^{-1} \equiv 1 \pmod n$. We say that a^{-1} is the inverse of $a \pmod n$.

The modular inverse is defined if and only if $\gcd(a, n) = 1$.

We can treat inverses as fractions - for instance, $\frac{1}{2} + \frac{1}{3} + \frac{1}{6} \equiv 1 \pmod p$ for $p \neq 2, 3$. The proof is non-trivial and inverses should be treated with care, so we will prove that all of these operations are valid.

You should rewrite all of these operations into fractions to understand what they're really saying. The proofs follow directly from the associative, distributive, and commutative properties.

Adding Inverses. For integers a, b relatively prime to n, $a^{-1} + b^{-1} \equiv (a + b)(ab)^{-1} \pmod n$.

Proof. Note that $(a + b)(ab)^{-1} \equiv aa^{-1}b^{-1} + ba^{-1}b^{-1} \equiv b^{-1} + a^{-1} \pmod n$.

Multiplying Inverses. For integers a, b relatively prime to n, $a^{-1}b^{-1} \equiv (ab)^{-1} \pmod n$.

Proof. Note that $(ab)^{-1}ab \equiv 1 \pmod n$ and $a^{-1}b^{-1}(ab) \equiv aa^{-1}bb^{-1} \equiv 1 \pmod n$.

Here is an example that uses the fact that modular inverses exist.

Example. How many ordered quadruplets of integers (a, b, c, d) with $1 \leq a, b, c, d \leq 4$ exist such that $5 \mid ab - cd$?

Solution. Note that this implies $ab \equiv cd \pmod{5}$, or $\frac{ab}{c} \equiv d \pmod{5}$. Notice that a choice of (a, b, c) will uniquely determine d, so the answer is just the number of ways to choose (a, b, c), or $4^3 = 64$ ways.

Make sure you understand **why** d is uniquely determined!

One last example, that uses purely standard modular arthimetic techniques; it epitomizes the ideas of this section. This is also an exercise in reading the problem carefully, and many students did overzealous approaches, for example bashing through all the cases. Unfourtunately, the answer was E, so this took a lot of time.[3]

Example (AMC 10B 2017/25). Last year Isabella took 7 math tests and received 7 different scores, each an integer between 91 and 100, inclusive. After each test she noticed that the average of her test scores was an integer. Her score on the seventh test was 95. What was her score on the sixth test?

Solution. Let A be the average of the first 6 tests. We know $6A + 95$ is a multiple of 7, as it is the sum of the first seven tests, or

$$6A + 95 \equiv 0 \pmod{7}.$$

This means we have $6A \equiv 3 \pmod{7}$, which means

$$A \equiv \frac{1}{2} \equiv \frac{8}{2} = 4 \pmod{7}.$$

However, A must be one of $91, 92, \dots, 100$. In fact we find $A = 95$. If the sixth score is S and the average of the first 5 tests is B, then since $570 = S + 5B$, S is multiple of 5 and must be **100**.

3 Chinese Remainder Theorem

The Chinese Remainder Theorem tells you that

1. given an independent system of linear congruences, you can "stitch them together" to one linear congruence that encompasses all of the conditions. This is often used when you obtain two mod conditions that are disjoint into one big condition that is easier to work with. In particular, finding values satisfying two linear congruences is hard, but finding values satistfying one modular congruence means one simply has to work with an arithmetic sequence.

2. given a linear congruence, you can "take it apart" into an independent system of linear congruence that encompasses the original congruence, and solve them independently. This is often used to split up a residue mod a composite number into residues mod prime powers, that are usually much more tolerable, and then using the previous to "put them back together" to find a exact value. For example, one might want to find the last three digits of a large number N. What one would do is find $N \pmod{8}$ and $N \pmod{125}$, then combine them to find $N \pmod{1000}$.

We state the formal theorem just to show that in of itself, it is completely devoid of any substance.

Chinese Remainder Theorem. For pairwise relatively prime positive integers $n_1, n_2, \dots, n_k$, a mod $n_1 n_2 \cdots n_k$ uniquely determines a mod n_i for $1 \le i \le k$, and vice versa.

Here is the following corollary that illustrates *how* to go about solving linear congruences.

[3] I (Ethan) seem to recall simply getting it wrong. Oops.

CRT Congruences. If $a \equiv b \pmod{p_i^{e_i}}$ for $1 \le i \le k$, then

$$a \equiv b \pmod{p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}}.$$

You'll notice that a common theme with the examples that use CRT Congruences is that it feels like we're rigging the congruences to work this way. That's because we are, and for small enough numbers, guesswork is sufficient.[4]

Here are some basic (and almost insultingly obvious) examples to underscore that the Chinese Remainder Theorem is just formalized intuition.

Example (Dominick Yeo). Prove that all integer arithmetic progressions with common difference 7 must contain multiples of 3.

This is not even technically CRT, but the idea is very similar to how "stitching" is done when given a concrete set of numbers to stich.

Solution. Say that the first term is a. Then there must be a solution to $a + 7k \equiv a + k \pmod 3$, and said solution is $k \equiv -a \pmod 3$.

Example. If the remainder of n is 1 when divided by 2 and n is divisible by 3, find its remainder when divided by 6.

Solution. Note that $n \equiv 1 \equiv 3 \pmod 2$ and $n \equiv 0 \equiv 3 \pmod 3$, so $n \equiv 3 \pmod 6$ by CRT Congruences.

Note that negative remainders also work, so use them whenever you see fit.

Example (Negative Remainders). Say the remainder of a number n is

$$\begin{aligned}&6 \text{ when divided by } 7,\\ &7 \text{ when divided by } 8, \text{ and}\\ &8 \text{ when divided by } 9.\end{aligned}$$

Find the remainder of n when divided by 504.

Solution. First note that $504 = 7 \cdot 8 \cdot 9$, and $7, 8, 9$ are pairwise relatively prime.

Now note that

$$\begin{aligned} n &\equiv 6 \equiv -1 \pmod 7\\ n &\equiv 7 \equiv -1 \pmod 8\\ n &\equiv 8 \equiv -1 \pmod 9,\end{aligned}$$

and CRT Congruences implies $n \equiv -1 \equiv 503 \pmod{504}$, so the remainder is 503.

Here are two much harder examples of the Chinese Remainder Theorem and CRT Congruences.

Example (AIME I 2014/8). The positive integers N and N^2 both end in the same sequence of four digits $abcd$ when written in base 10, where digit a is not zero. Find the three-digit number abc.

[4] There is an algorithm, but it is sufficiently easy to just work out yourself, alongside the Euclidean Algorithm.

Solution. Note that by the Chinese Remainder Theorem,

$$N^2 \equiv N \pmod{16}$$

$$N^2 \equiv N \pmod{625}.$$

This implies that

$$N(N-1) \equiv 0 \pmod{16}$$

$$N(N-1) \equiv 0 \pmod{625}.$$

Ignoring the restriction of $a \neq 0$, we can have $N \equiv 0, 1 \pmod{16}$ and $N \equiv 0, 1 \pmod{625}$, resulting in 4 overall systems of congruences to solve.

Obviously $N \equiv 0 \pmod{16}$ and $N \equiv 0 \pmod{625}$ leads to $N \equiv 0 \pmod{10000}$, and $N \equiv 1 \pmod{16}$ and $N \equiv 1 \pmod{625}$ leads to $N \equiv 1 \pmod{10000}$, so they aren't what we're looking for.

We try $N \equiv 1 \pmod{16}$ and $N \equiv 0 \pmod{625}$. To find the value of N that will make CRT Congruences work, we are trying to find $N \equiv 625n \pmod{625}$ such that $625n \equiv 1 \pmod{16}$. Note that $625n \equiv n \equiv 1 \pmod{16}$, implying that $n = 1$ will suffice, leaving us with $N \equiv 625 \pmod{16}$ and $N \equiv 625 \pmod{625}$, or $N \equiv 625 \pmod{10000}$. This has $a = 0$, so it isn't what we're looking for.

We now try $N \equiv 0 \pmod{16}$ and $N \equiv 1 \pmod{625}$. To find the value of N that will make CRT Congruences work, we are trying to find $N \equiv 625n + 1 \pmod{625}$ such that $625n + 1$ is divisible by 16. Note that $625n + 1 \equiv n + 1 \pmod{16}$, so $n = 15$ will suffice, leaving us with

$$N \equiv 16 \cdot 586 \equiv 9376 \pmod{16}$$

$$N \equiv 625 \cdot 15 + 1 \equiv 9376 \pmod{625},$$

or $N \equiv 9376 \pmod{10000}$. So the answer is 937.

Example (AMC 10A 2020/24). Let n be the least positive integer greater than 1000 for which

$$\gcd(63, n + 120) = 21 \quad \text{and} \quad \gcd(n + 63, 120) = 60.$$

What is the sum of the digits of n?

A somewhat pedagogical and unrelated comment: the problem asks for the sum of the digits of n because otherwise you could game the problem by just trying all of the answer choices. In this case, the problem does not imply that finding the sum of the digits of n as opposed to finding n will solve the problem in a quicker or easier way. This sort of approach does humorously work sometimes, and is a tip for guessing.

Solution. Our gcd equations give us possible remainders of n when divided by 63 and 120, which clues us in to the Chinese Remainder Theorem. In particular, we know we are going to want to put them together into one big congruence, as $n > 1000$.

Note that $n + 120 \equiv 0 \pmod{21}$, or $n \equiv 6 \pmod{21}$, but also note that $n \not\equiv 6 \pmod{63}$. Thus $n \equiv 27 \pmod{63}$ or $n \equiv 48 \pmod{63}$. Similarly, $n \equiv 117 \pmod{120}$. This gives us two possible systems of congruences.

The first system is

$$n \equiv 27 \pmod{63}$$

$$n \equiv 117 \pmod{120}.$$

Note that the factor of 3 is redundant in the second congruence, as this is equivalent to

$$n \equiv 0 \pmod{9}$$

$$n \equiv 6 \pmod{7}$$
$$n \equiv 3 \pmod{8}$$
$$n \equiv 2 \pmod{5},$$

so it is equivalent to

$$n \equiv 27 \pmod{63}$$
$$n \equiv 37 \pmod{40}.$$

Note that we want to solve the system

$$n \equiv 63a + 27 \pmod{63}$$

$$n \equiv 63a + 27 \equiv 23a + 27 \equiv 37 \pmod{40}.$$

Now we just sensibly add multiples of 23 and pray that $23a + 30$ becomes divisible by 40. This occurs when $a = 30$, so

$$n \equiv 63a + 27 \equiv 63 \cdot 30 + 27 \equiv 1917 \pmod{2520}.$$

So the smallest n in this system is $n = 1917$.

The second system proceeds similarly – we spare the details because it's very similar to the first one. Note that

$$n \equiv 48 \equiv 237 \pmod{63}$$
$$n \equiv 37 \equiv 237 \pmod{40},$$

so $n \equiv 237 \pmod{2520}$. But $237 < 1000$, so the smallest n is $n = 237 + 2520 = 2757$. So the minimum is 1917, and the answer is $1 + 9 + 1 + 7 = 18$.

4 Fermat's Little Theorem

Often in number theory problems we will want to take some number to some large power and find its remainder when divided by another number. Fermat's Little Theorem provides a way to make this calculation much easier.

Fermat's Little Theorem. Consider a prime p. For any integer a, $a^p \equiv a \pmod{p}$.

If we add the restriction that a and p are relatively prime, we can divide by a on both sides to achieve the following.

Fermat's Little Theorem, alternative. Consider a prime p. For relatively prime a, p, $a^{p-1} \equiv 1 \pmod{p}$.

There are two proofs for this theorem. We present the induction proof first because it requires the least amount of ingenuity.

Proof 1 (Induction). For the inductive proof, we prove that $a^p \equiv a \pmod{p}$.

This is obviously true for the base case $a = 1$.

Now assume that this is true for $a = n$. Then

$$(n+1)^p \equiv n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + 1 \pmod{p}.$$

But notice that $\binom{p}{1}, \binom{p}{2} \ldots \binom{p}{p-1}$ are all divisible by p, so

$$n^p + \binom{p}{1} n^{p-1} + \binom{p}{2} n^{p-2} + \cdots + 1 \equiv n^p + 1 \equiv n + 1 \pmod{p},$$

as desired.

The rearrangement proof requires a little bit more creativity and is more aesthetic. It can also be generalized to Euler's Theorem, where the first proof cannot.

Proof 2 (Rearrangement). Suppose that a and p are relatively prime. We claim that $a, 2a, 3a \ldots a(p-1)$ is a rearrangement of $1, 2, 3 \ldots p-1$ taken mod p. We prove this by contradiction. Assume that there are two integers such that $ax \equiv ay \pmod{p}$ with $0 < x, y < p$ and $x \neq y$. Since $\gcd(a, p) = 1$, we can divide both sides by a to yield $x \equiv y$. But this is obviously not possible. Thus, contradiction.

This implies that $(p-1)! \equiv a^{p-1}(p-1)! \pmod{p}$. As $\gcd(p, (p-1)!) = 1$, we can divide both sides by $(p-1)!$ to get $1 \equiv a^{p-1} \pmod{p}$, as desired.

Here are some basic examples of Fermat's Little Theorem.

Example. Find the remainder of $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60}$ when divided by 7.

Solution. Note that

$$\begin{aligned} 2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} &\equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0 \\ &\equiv 4 + 1 + 256 + 25 + 1 \\ &\equiv 0 \pmod{7}. \end{aligned}$$

Example (AMC 12A 2008/15). Let $k = 2008^2 + 2^{2008}$. What is the units digit of $k^2 + 2^k$?

Solution. This is a mixture of Chinese Remainder Theorem and Fermat's Little Theorem.

Obviously $2 \mid k^2 + 2^k$, so we can consider its remainder when divided by 5. Now note that

$$k \equiv 2008^2 + 2^{2008} \equiv 3^2 + 2^0 \equiv 0 \pmod{5}.$$

Since $5 \mid k$ and $4 \mid k$,

$$k^2 + 2^k \equiv 2^k \equiv 1 \pmod{5}.$$

Now by CRT Congruences,

$$\begin{aligned} 0 &\equiv 6 \pmod{2} \\ 1 &\equiv 6 \pmod{5}, \end{aligned}$$

so the remainder when divided by 10 is 6 as well.

Here's a pedagogical example of Fermat's and Chinese Remainder Theorem.

Example (42 PMO Level 3 2020/1). Let $p_1, p_2, \dots, p_n$ be distinct prime numbers and P be their product. Let the number S be defined as

$$S = \sum_{i=1}^{n} \left(\frac{P}{p_i} \right)^{p_i - 1}.$$

Show that $S - 1$ is a multiple of P.

Solution. Note that $S \equiv \left(\frac{P}{p_k} \right)^{p_k - 1} \equiv 1 \pmod{p_k}$ by Fermat's Little Theorem, so $S \equiv 1 \pmod{P}$ by CRT.

4.1 Monic Monomials mod n

The important idea is that monic monomials **don't always cover all residues** mod n for certain n.

We begin with perhaps the most famous and often used example.

Example (Quadratic Residues mod 4). The only positive integers $0 \le k < 4$ such that $n^2 \equiv k \pmod 4$ has a solution are $k = 0$ and $k = 1$.

In other words, the remainder of a square divided by 4 is always 0 or 1.

Solution. Just plug in $0, 1, 2, 3$ and check only $0, 1$ are outputted.

Example (Macedonia JBMO TST 2016/1). Solve

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 = 2016^3 - 1$$

over the integers.

Solution. There are no solutions. Take mod 16 and note that $x^4 \in \{0, 1\} \pmod{16}$ and $2016^3 - 1 \equiv 15 \pmod{16}$.

With practice and experience, these patterns will become clearer over time. For instance, fourth powers strongly suggest taking mod 16, and squares strongly suggest taking mod 4, mod 3, or mod 8, depending on the context.

Speaking of squares and mod 3 . . .

Example (USAJMO 2011/1). Find, with proof, all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.

Solution. We claim the only solution is $n = 1$, since $2 + 12 + 2011 = 2025 = 45^2$.

Now we claim that no solutions $n > 1$ work. Assume otherwise. Then note that for mod 3 reasons, we must have n be odd since $2^n + 2011^n \equiv 2^n + 1^n \equiv 2^n + 1 \pmod 3$, and we must have it be congruent to 0 mod 3. But also note for mod 4 reasons, we must have n be even since $2011^n \equiv (-1)^n \pmod 4$, and we must have it be congruent to 1 mod 4, contradiction.

4.2 Exponential Functions mod n

You will also want to consider exponential functions mod n. The idea is you can use Fermat's Little Theorem to figure out the residues the function is restricted to.

We start with an easier problem as an example.

Example (April USAJMO 2020/1). Determine, with proof, whether there exists a positive integer n such that $4^n - 1$ divides $5^n - 1$.

Solution. Clearly $3 \mid 4^n - 1$ so we must have $3 \mid 5^n - 1$, implying that $2 \mid n$. But also note that $2 \mid n$ implies $5 \mid 4^n - 1$, contradiction.

Exponential functions usually go hand in hand with bounding and size arguments.

Example (TurtleKing123). Find all ordered triplets of natural numbers (a, b, c) such that

$$6^a + 7^b = 13^c.$$

The proof of the $a = 1$ case is better suited for the Prime Factorization unit, but the rest is quite informative for this unit.

Solution. We claim the answer is just $a = b = c = 1$, and it is easy to check that it works.

Assume $a > 2$. The cases $a = 1$ and $a = 2$ will be shown later.

Taking mod 4 gives us that b is even, and then taking mod 8 gives c is even as well. Let $2x = b$ and $2y = c$. Then

$$(13^x - 7^y)(13^x + 7^y) = 6^a.$$

Note that for mod 3 reasons all powers of 3 are concentrated in $13^x - 7^y$, so $13^x + 7^y$ must be of the form 2^k. But this implies that $3^k \mid 13^x - 7^y$, absurd for size reasons.

For $a = 2$ note that taking mod 14 gives that b is even and c is odd, but mod 14 gives that b is odd and c is even, contradiction.

For $a = 1$, subtract 13 to get

$$7^b - 7 = 13^c - 13.$$

The first main claim is that $43 \mid 7^b - 7$. Note that $12 \mid b - 1$ since the smallest number k such that $7^k \equiv 1 \pmod{13}$ is 12, so $43 \mid 7^{12} - 1 \mid 7^b - 7$.

The second main step is proving $14 \mid c - 1$. Note that $7 \mid k$ where k is the smallest number such that $13^k \equiv 1 \pmod{43}$, since $13^6 \equiv 6 \pmod{43}$, implying $7 \mid c - 1$. Also for mod 7 reasons, $2 \mid c - 1$, which implies that $14 \mid c - 1$. Then note that by LTE, $49 \mid 13^{14} - 1$, so $49 \mid 13^c - 13$. Thus $49 \mid 7^b - 7$, which is only possible if $b = 1$.

Now we present a much harder example. If you don't know what the order of a number modulo a prime is, the idea is that $\text{ord}_p\, n$ is the smallest integer k such that $n^k \equiv 1 \pmod{p}$.[5]

Example (SJMO 2020/1). Find all positive integers $k \geq 2$ for which there exists some positive integer n such that the last k digits of the decimal representation of $10^{10^n} - 9^{9^n}$ are the same.

Solution. We claim only $2 \leq k \leq 4$ works. It suffices to just provide a construction for $k = 4$, and said construction is $n = 25$. We verify this works later in the proof.

We show that the only way to have the last two digits be the same is for them to both be 11. Note

$$10^{10^n} - 9^{9^n} \equiv -9^{9^n} \equiv -1 \pmod{4}$$

[5] I also recommend you skip this example for now if you don't know what order is.

$$10^{10^n} - 9^{9^n} \equiv -9^{9^n} \pmod{25}.$$

Now note that $9^{10} \equiv 1 \pmod{25}$ by Euler's Theorem, so $9^{9^n} \equiv 9^{(-1)^n} \equiv 9, 14 \pmod{25}$. Thus the only possible remainders of -9^{9^n} divided by 100 are $-9, -89$, or $91, 11$. So 11 is the only possible ending 2 digits.

Now this implies we want to solve $10^{10^n} - 9^{9^n} \equiv -9^{9^n} \equiv 10^0 + 10^1 + \cdots + 10^{k-1} \pmod{10^k}$. This is valid because if $10^{10^n} \le 10^{k-1}$ this is obviously not true. In other words,

$$9^{9^n} \equiv 8(10^0 + 10^1 + \cdots + 10^{k-1}) + 1 \equiv \frac{8(10^k - 1)}{9} + 1 \equiv \frac{1}{9} \pmod{10^k},$$

or $9^{9^n+1} \equiv 1 \pmod{10^k}$.

Now we show that $n = 25$ works for $k \ge 4$. Note that the smallest number k such that $3^k \equiv 1 \pmod{2^4}$ is $k = 4$, and $4 \mid 2(9^{25} + 1)$ and $\phi(5^4) = 4 \cdot 5^3$, and $4 \cdot 5^3 \mid 2(9^{25} + 1)$, where $4 \mid 2(9^{25} + 1$ is obvious and $5^3 \mid 9^{25} + 1$ follows from LTE as $\nu_5(9^{25} + 1) = \nu_5(9 + 1) + \nu_5(25) = 3$.

Now we prove $k > 4$ doesn't work. Note that the minimal k such that $3^k \equiv 1 \pmod{2^5}$ is $k = 8$, and $8 \nmid 2(9^n + 1)$ as $9^n + 1 \equiv 2 \pmod 4$. Thus there are no solutions to $9^{9^n+1} \equiv 1 \pmod{2^k}$ for $k > 4$.

5 Euler's Totient Function

Now we take a look at Euler's Totient Function.

Euler's Totient Function. We define $\phi(n)$ to be the number of positive integers less than or equal to n that are also relatively prime to n.

Multiplicativity. For relatively prime m, n, $\phi(m) \cdot \phi(n) = \phi(mn)$.

The basic idea of the proof is just using CRT to find all possible congruences.

Proof. Note that we can have

$$x \equiv j_1, j_2, \ldots, j_{\phi(m)} \pmod{m}$$
$$x \equiv k_1, k_2, \ldots, k_{\phi(n)} \pmod{n},$$

where j_i encompasses the numbers between 1 and m relatively prime to m and k_i encompasses the number between 1 and n relatively prime to n. Then note that this system has $\phi(m)\phi(n)$ solutions when taken mod mn.

Product Formula. Say the prime factorization of positive integer n is $p_1^{e_1} \cdot p_2^{e_2} \ldots p_k^{e_k}$. Then $\phi(n) = n\frac{p_1-1}{p_1} \cdot \frac{p_2-1}{p_2} \ldots \frac{p_k-1}{p_k}$.

Proof. Instead of actually proving this fully, we outline it for the reader to work through themselves.

1. Find $\phi(p_1^{e_1})$.

2. Use multiplicity to find $\phi(p_1^{e_1})\phi(p_2^{e_2}) \cdots \phi(p_k^{e_k})$.

Euler's Totient Theorem. For relatively prime a, n, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. This is very similar to the rearrangement proof for Fermat's Little Theorem.[6]

Let the set of positive integers less than and relatively prime to n be $x_1, x_2, \dots, x_{\phi(n)}$. Then note that $ax_1, ax_2, \dots, ax_{\phi(n)}$ is a rearrangement of $x_1, x_2, \dots, x_{\phi(n)}$.

We proceed by contradiction. Assume that there are two integers such that $ax \equiv ay \pmod{n}$. Since $\gcd(a, n) = 1$, we can divide both sides by a to yield $x \equiv y$. But this is obviously not possible. Thus, contradiction.

This implies that $x_1x_2\dots x_{\phi(n)} \equiv (x_1x_2\dots x_{\phi(n)})a^{\phi(n)} \pmod{n}$. Dividing both sides by $x_1x_2\dots x_{\phi(n)}$ yields $a^{\phi(n)} \equiv 1 \pmod{n}$, as desired.

Also, notice that Fermat's is just a special case of Euler's.

6 Wilson's Theorem

Factorials rarely appear in number theory (at least for the AMCs and the AIME). But Wilson's Theorem is still one of the standard tools you need to have at your disposal.

Wilson's Theorem. For prime p,

$$(p-1)! \equiv -1 \pmod{p}.$$

Proof 1. Notice that the numbers $2, 3, 4 \dots p-2$ all have modular inverses. In addition, modular inverses come in pairs. Since p is odd (the case where $p = 2$ is very easy to deal with), then the modular inverses all multiply to 1. This leaves us with $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$, as desired.

We do not include $1, p-1$ in the pairing because for prime p, 1 and $p-1$ are the only numbers whose modular inverses are themselves.

The following proof is much trickier and should not be focused on by people encountering modular arithmetic for the first time.

Proof 2. The crucial claim is that

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod{p}.$$

This is because $x^{p-1} \equiv 1 \pmod{p}$ for all x by Fermat's Little Theorem, and since we have found $p-1$ roots, there are clearly no more.

Now note that

$$0^{p-1} - 1 \equiv (-1)(-2)\cdots(-(p-1)) \equiv (p-1)! \pmod{p}$$

for all $p > 2$. The case $p = 2$ can be manually checked.

A corollary of this proof is that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$ for $p - 1 \nmid k$.

You can use Wilson's Theorem to deal with binomial coefficients mod p effectively.

Example. Show that $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for all $0 \le k \le p-1$.

[6] So similar, in fact, that I copy-pasted the proof for Fermat's and made minor adjustments.

Solution. Note that

$$\begin{aligned}\binom{p-1}{k} &\equiv \frac{(p-1)!}{k!(p-1-k)!} \\ &\equiv \frac{-1}{(-1)^k(p-k)(p+1-k)(p+2-k)\cdots(p+k-1-k)(p-1-k)!} \\ &\equiv \frac{-1}{(-1)^k(p-1)!} \\ &\equiv (-1)^k \pmod{p}.\end{aligned}$$

Wilson's theorem is actually kind of unnecessary here; note that $(p-1)!$ cancels.

As an exercise, find $\binom{p-2}{k} \pmod{p}$ in terms of p, k for $p > 2$.

7 Problems

Minimum is [54 ♟]. Problems denoted with ♞ are required. (They still count towards the point total.)

> "Take what fortune grants you, use it while you've got it!"
>
> Death Note Musical

[1 ♟] **Problem 1** Find the inverse of $2 \pmod{p}$ for odd prime p in terms of p.

[1 ♟] **Problem 2** Find the remainder of $97!$ when divided by 101.

[1 ♟] **Problem 3** Find the remainder of $(p-2)!$ when divided by p, provided that p is prime.

[2 ♟] **Problem 4 (AMC 12A 2003/18)** Let n be a 5-digit number, and let q and r be the quotient and the remainder, respectively, when n is divided by 100. For how many values of n is $q+r$ divisible by 11?

[2 ♟] **Problem 5 (MAST Diagnostic 2020)** How many integer values of $1 \le x \le 100$ makes x^2+8x+5 divisible by 10?

[2 ♟] **Problem 6 (1001 Problems in Number Theory)** For which positive integers n is it true that $1+2+\cdots+n \mid 1\cdot 2\cdot\cdots\cdot n$?

[2 ♟] **Problem 7** What is the residue of $\frac{1}{1\cdot2}\cdot\frac{1}{2\cdot3}\cdot\cdots\cdot\frac{1}{11\cdot12} \pmod{13}$?

[2 ♞] **Problem 8 (AMC 10A 2020/18)** Let (a,b,c,d) be an ordered quadruple of not necessarily distinct integers, each one of them in the set $0,1,2,3$. For how many such quadruples is it true that $a\cdot d - b\cdot c$ is odd? (For example, $(0,3,1,1)$ is one such quadruple, because $0\cdot1-3\cdot1=-3$ is odd.)

[3 ♟] **Problem 9 (AMC 10B 2018/16)** Let $a_1, a_2, \dots, a_{2018}$ be a strictly increasing sequence of positive integers such that

$$a_1+a_2+\cdots+a_{2018} = 2018^{2018}.$$

What is the remainder when $a_1^3+a_2^3+\cdots+a_{2018}^3$ is divided by 6?

[3 ♟] **Problem 10 (PUMaC 2018)** Find the number of positive integers $n < 2018$ such that 25^n+9^n is divisible by 13.

[3 ♟] **Problem 11** Prove $\phi(n)$ is composite for $n \ge 7$.

[3 ♟] **Problem 12 (AMC 10B 2019/14)** The base-ten representation for $19!$ is $121,6T5,100,40M,832,H00$, where T, M, and H denote digits that are not given. What is $T+M+H$?

[4 ♟] **Problem 13** Find the remainder of $5^{31}+5^{17}+1$ when divided by 31.

[4 ♟] **Problem 14 (OMO 15-16 Spring/9)** Let $f(n) = 1\times3\times5\times\cdots\times(2n-1)$. Compute the remainder when $f(1)+f(2)+f(3)+\cdots+f(2016)$ is divided by 100.

[4 ♟] **Problem 15** Prove that the equation $x^2+y^2+z^2 = x+y+z+1$ has no solutions over the rationals.

[4 ♞] **Problem 16 (MAST Diagnostic 2021)** Find the remainder of $(1^3)(1^3+2^3)(1^3+2^3+3^3)\dots(1^3+2^3+3^3\cdots+99^3)$ when divided by 101.

[6 ♟] **Problem 17 (Wolstenholme's Theorem)** Prove that for all prime $p \ge 5$, we have $p^2 \mid (p-1)!\left(\sum_{i=1}^{p-1}\frac{1}{i}\right)$.

[6 ♟] **Problem 18 (AIME 1989/9)** One of Euler's conjectures was disproved in the 1960s by three American mathematicians when they showed there was a positive integer such that $133^5+110^5+84^5+27^5=n^5$. Find the value of n.

[6 ♟] Problem 19 (USAMO 1979/1) Determine all non-negative integral solutions $(n_1, n_2, \ldots, n_k)$, if any, apart from permutations, of the Diophantine equation

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599.$$

[6 ♟] Problem 20 (AIME II 2017/8) Find the number of positive integers n less than 2017 such that

$$1 + n + \frac{n^2}{2!} + \frac{n^3}{3!} + \frac{n^4}{4!} + \frac{n^5}{5!} + \frac{n^6}{6!}$$

is an integer.

[6 ♟] Problem 21 (IMO 1970/4) Find all positive integers n such that the set $\{n, n+1, n+2, n+3, n+4, n+5\}$ can be partitioned into two subsets so that the product of the numbers in each subset is equal.

[6 ♟] Problem 22 (AIME I 2001/11) In a rectangular array of points, with 5 rows and N columns, the points are numbered consecutively from left to right beginning with the top row. Thus the top row is numbered 1 through N, the second row is numbered $N + 1$ through $2N$, and so forth. Five points, P_1, P_2, P_3, P_4, and P_5, are selected so that each P_i is in row i. Let x_i be the number associated with P_i. Now renumber the array consecutively from top to bottom, beginning with the first column. Let y_i be the number associated with P_i after the renumbering. It is found that $x_1 = y_2$, $x_2 = y_1$, $x_3 = y_4$, $x_4 = y_5$, and $x_5 = y_3$. Find the smallest possible value of N.

[9 ♟] Problem 23 (IMO 2005/4) Determine all positive integers relatively prime to all the terms of the infinite sequence

$$a_n = 2^n + 3^n + 6^n - 1,\ n \geq 1.$$

[13 ♟] Problem 24 (AIME I 2013/15) Let N be the number of ordered triples (A, B, C) of integers satisfying the conditions

- $0 \leq A < B < C \leq 99$,
- there exist integers a, b, and c, and prime p where $0 \leq b < a < c < p$,
- p divides $A - a$, $B - b$, and $C - c$, and
- each ordered triple (A, B, C) and each ordered triple (b, a, c) form arithmetic sequences.

Find N.

[13 ♟] Problem 25 (USEMO 2019/4) Prove that for any prime p, there exists a positive integer n such that

$$1^n + 2^{n-1} + 3^{n-2} + \cdots + n^1 \equiv 2020 \pmod{p}.$$

7.1 Period of a Repeating Decimal

[2 ♟] Problem 26 The expansion of $\frac{1}{7}$ is $0.\overline{142857}$, which is a repeating decimal with a 6 digit long sequence. How many digits long is the expansion of $\frac{1}{13}$?

[3 ♟] Problem 27 We define the cycle of a repeating fraction $\frac{m}{n}$ as the minimum number i such that $\frac{m}{n} = 0.\overline{a_1 a_2 a_3 \ldots a_i}$. Find the cycle of $\frac{1}{23}$.

[3 ♟] **Problem 28 (AMC 10A 2019/18)** For some positive integer k, the repeating base-k representation of the (base-ten) fraction $\frac{7}{51}$ is $0.\overline{23}_k = 0.232323\ldots_k$. What is k?

[4 ♞] **Problem 29 (e-dchen Mock MATHCOUNTS)** What is the sum of all odd n such that $\frac{1}{n}$ expressed in base 8 is a repeating decimal with period 4?

[6 ♟] **Problem 30 (AMC 12A 2014/23)** The fraction

$$\frac{1}{99^2} = 0.\overline{b_{n-1}b_{n-2}\ldots b_2b_1b_0},$$

where n is the length of the period of the repeating decimal expansion. What is the sum $b_0 + b_1 + \cdots + b_{n-1}$?

[6 ♟] **Problem 31 (AMC 12B 2016/22)** For a certain positive integer n less than 1000, the decimal equivalent of $\frac{1}{n}$ is $0.\overline{abcdef}$, a repeating decimal of period 6, and the decimal equivalent of $\frac{1}{n+6}$ is $0.\overline{wxyz}$, a repeating decimal of period 4. Find n.