Week 6 Intermediate: Modular Arithmetic II

Math Divulged

June 17, 2020

§1 Introduction

This handout will assume you are at least mildly familiar with the introductory handout and the concepts of modular arithmetic. Some of the content will be repetitive, but there will be a greater emphasis on proofs and the insight and motivation driving the logic and reasoning.

Aside from several basic theorems and tricks, modular arithmetic struggles to really make an impact on the competition field at the AMC and AIME level. Many seemingly number theoretical problems at a computational level are actually combinatorial. Furthermore, the amount of number theory problems in these competitions is few in comparison to other subjects. That's not to say advanced computational problems don't exist, but they are never difficult given sufficient experience in NT. I'll use this course to briefly give an idea of what ideas and concepts appear in higher level number theory, especially where proofs are more valued.

Several main themes will repeatedly appear in this lesson, but we'll categorize this handout by topic.

§2 Linear Congruences

As mentioned in the introductory lecture, modular congruence can be interpreted as the remainder when divided by the mod. Two numbers with the same remainder are congruent.

Definition 2.1. For integers a, b and positive integer n, we have

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

if and only if $n \mid a - b$.

It's easy to observe that the common properties for ordinary equivalence hold for congruences with the exception of division. Thus, in order to solve linear congruence equations like $ax + b \equiv c \pmod{n}$, we are in need of an analogy to division.

§2.1 Multiplicative Inverses

When we divide a number x by y, we are essentially multiplying x by y's multiplicative inverse, which is $y^{-1} = 1/y$. The inverse satisfies $y \cdot y^{-1} = 1$. So, we should look for a similar number in modular arithmetic.

Definition 2.2. The number b is called a multiplicative inverse of a modulo n if

$$ab \equiv 1 \pmod{n}.$$

We usually write $a^{-1} = b$.

It's easy to observe that a number like 8 (mod 15) has an inverse of 2 while a number like 3 (mod 15) has no possible inverse. We can conclude that there doesn't always exist an inverse, but there should be a method to identify when an inverse exists. To approach this, we'll introduce a theorem seemingly unrelated to mods.

Theorem 2.3 (Bezout)
For any positive integers a, b, there exists integers x, y such that $ax + by = \gcd(a, b)$.

One proof for this involves the set S of numbers of the form $ax + by$ and an argument involving the minimal element of S. You can try to prove this theorem on your own.

We can use Bezout to not only demonstrate when an inverse exists, but also as a hint on how to compute an inverse algorithmically.

Theorem 2.4
For an integer a, there exists an integer a^{-1} such that

$$a \cdot a^{-1} \equiv 1 \pmod{n}$$

if and only if a and n are relatively prime, that is, $\gcd(a, n) = 1$.

Proof. If an inverse $a^{-1} = b$ exists, then we can write $ab = 1 + nx$ for some integer x. This can be rearranged into

$$1 = ab - nx = \gcd(a, -n) = \gcd(a, n)$$

using Bezout's identity. The converse statement follows in reverse, starting with Bezout. □

It's important to remember that when proving an "if and only if" statement, you must prove both directions of the statement. The proof above was fairly simple to where it's obvious on how the converse can be proven.

Since Bezout tells us that there exists an integer b such that $ab - nx = \gcd(a, n)$ for relatively prime a, n, we can use this to our advantage. The Euclidean Algorithm used for computing the GCD of a number uses a and n to compute the GCD, and by tracking the coefficients used to reach a value of 1, we can easily determine what $b = a^{-1}$ is. This is called the **Extended Euclidean Algorithm**.

Modular arithmetic can actually play into GCD's as well.

Theorem 2.5
If $a \equiv b \pmod{n}$, then $\gcd(a, n) = \gcd(b, n)$.

Proof. Using the definition of a congruence, $a = nk + b$ for some integer k. So,

$$\gcd(a, n) = \gcd(nk + b, n) = \gcd(b, n).$$

□

This makes sense, because finding the remainder after division is essentially what the Euclidean Algorithm aims to do.

Inverses offer a practical way to form the number 1 in multiplication, and this can be used to our advantage in certain problems.

Example 2.6

For an odd positive integer $n > 1$, let S be the set of integers x, $1 \leq x \leq n$, such that both x and $x + 1$ are relatively prime to n. Show that

$$\prod_{x \in S} x \equiv 1 \pmod{n}.$$

Solution. The congruence to 1 should be a mild hint that perhaps the solution involves using inverses. If we could potentially pair each number x and $x + 1$ with their inverses, the product would hold. So, we should aim on proving that the set S contains pairs of inverses.
Let x be an element of S. We know that since $x \cdot x^{-1} \equiv 1 \pmod{n}$, so using Theorem 2.5,

$$\gcd(xx^{-1}, n) = \gcd(1, n) = 1.$$

Furthermore, since x and n share no common factors,

$$\gcd(x^{-1}, n) = \gcd(xx^{-1}, n) = 1$$

and so x^{-1} is also relatively prime to n. If we can show that $x^{-1} + 1$ is also relatively prime to n, then we know that x^{-1} is also an element of the set S. Since $x(x^{-1}+1) \equiv x+1 \pmod{n}$, Theorem 2.5 tells us that

$$\gcd(x(x^{-1} + 1)) = \gcd(x + 1, n) = 1.$$

We know that x shares no common factors with n, so

$$\gcd(x^{-1} + 1, n) = \gcd(x(x^{-1} + 1)) = 1$$

and therefore, $x^{-1} + 1$ is also coprime to n and by the definition of S, we know that x^{-1} is also an element.
Now we have to check if there is a case where $x = x^{-1}$. Assume that there exists a case, so $\gcd(x + 1, n) = 1$. Since $x^2 \equiv 1 \pmod{n}$, We have $x^2 + 2x + 1 \equiv 2(x + 1) \pmod{n}$ and since $x + 1$ is coprime to n, there exists an inverse. Multiplying the inverse to both sides gives $x + 1 \equiv 2 \pmod{n}$ which implies only $x = 1$ is possible.
Thus, if we pair each x in S with its inverse, their overall product is $1 \pmod{n}$. □

This is definitely not a simple problem you'd encounter frequently in competitions, but it was simple if you knew to pair inverses with one another. To do this, we had to show that the inverse of an element of S was also in S. Furthermore, to ensure that our product of pairs did not overcount a case where $x = x^{-1}$, we encountered what seemed like a quadratic congruence. However, the circumstances allowed us to reduce it safely to a linear congruence using inverses.

§2.2 System of Congruences

This had already been addressed in the introductory handout, but it'll be included here for completeness.

Theorem 2.7 (Chinese Remainder Theorem)

If $m_1, ..., m_n$ are pairwise relatively prime, then the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\dots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a solution modulo $m_1 m_2 \cdot ... \cdot m_n$.

In terms of usage in proofs, CRT is primarily used to prove that a specific solution or value exists. For an example of solving a system of congruences, see the introductory handout.

§3 Exponential Congruences

In the introductory handout, we discussed how to compute exponential terms using several tricks and theorems. Here, we will emphasize more on the methods used in proving these theorems.

§3.1 Binomials

Binomials and exponents have a lot in common.

Theorem 3.1

For a prime p, $\binom{p}{k} \equiv 0 \pmod{p}$ for all $1 \leq k \leq p-1$.

Proof. The binomial coefficient may be expanded into its factorial form, and the denominator contains no multiple of p but the numerator does. Hence, p must divide it. □

This can be used with binomial expansion to produce an interesting result.

Theorem 3.2

For two integers a, b and prime p, $(a+b)^p \equiv a^p + b^p \pmod{p}$.

Proof. By Binomial Expansion,

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$$

and since $p \mid \binom{p}{k}$ by Theorem 3.1 for all $1 \leq k \leq p-1$, we have that in modulo p, all terms but $a^p + b^p$ reduce to $0 \pmod{p}$. □

This is a neat trick which can be generalized further with induction. **Induction** is a technique in proofs where we assume a statement is true and then prove the next iteration of the statement using the assumed statement. Teachers often relate it to dominoes.

Theorem 3.3 (Freshmen's Exponentiation)

For integers $a_1, ..., a_n$ and prime p, we have

$$(a_1 + ... + a_n)^p \equiv a_1^p + ... + a_n^p \pmod{p}.$$

Proof. We proceed with induction. **Base Case:** $n = 2$. This is true by Theorem 3.2. Now assume the theorem is true for $a_1, a_2, ..., a_n$. Then we have

$$((a_1 + ... + a_n) + a_{n+1})^p \equiv (a_1 + ... + a_n)^p + a_{n+1}^p \pmod{p}$$

by Theorem 3.2 again, and by inductive hypothesis,

$$(a_1 + ... + a_n)^p \equiv a_1^p + ... + a_n^p \pmod{p}.$$

Hence, we have completed our induction. □

The name for this theorem comes from the stereotypical freshmen, who, not knowing binomial expansion, assumes this is equal outside of modular arithmetic.

§3.2 Three Little Theorems

The following three theorems are widely used in modular arithmetic, especially at a more basic level.

Theorem 3.4 (Fermat's Little Theorem)

For a prime p and integer a,

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

Proof. We proceed by induction. **Base Case:** $a = 1$. Then $1^p \equiv 1 \pmod{p}$ and the statement holds true.
Now assume the statement is true for a. It is clear that $(a + 1)^p \equiv a^p + 1 \pmod{p}$ by Theorem 3.2 and by hypothesis of induction (we assume $a^p \equiv a \pmod{p}$), we have $a^p + 1 \equiv a + 1 \pmod{p}$ as desired and our induction is complete. □

The following theorem uses a pairing strategy similar to Example 2.6.

Theorem 3.5 (Wilson)

For a prime p, we have

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

Proof. Note that for all numbers in the range 2 to $p - 2$, there exists a multiplicative inverse in the same range. We know that there is no case where an integer k in this range satisfies $k = k^{-1}$ due to the same reasoning from Example 2.6. Therefore, multiplying all these pairs together gives $(p-2)! \equiv 1 \pmod{p}$ and so, $(p-1)! \equiv p-1 \equiv -1 \pmod{p}$. □

The following theorem uses a strategy of running through the elements of a set. First, we need to define a relevant function.

Definition 3.6. The totient function $\phi(n)$ is equal to the number of integers less than n that are relatively prime to n.

Theorem 3.7 (Euler)
Given two relatively prime integers a and n,

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

Proof. Let us first look at the behavior of coprime numbers with respect to n. When multiplying two numbers a, b both coprime to n together, you get another number coprime to n. Let the set S consist of numbers from 1 to n that are coprime to n. Multiplying a to two different elements r_1, r_2 of S produces two different values ar_1, ar_2. If $ar_1 \equiv ar_2 \pmod{n}$, we can use the inverse of a to show $r_1 = r_2$. Thus, if we multiply all the elements in S by $a \pmod{n}$ to create set S', the new set is exactly identical in elements to S. Note that there are $\phi(n)$ elements in S.
Let P, P' be the product of all the elements in S, S', respectively. P and P' are both coprime with n. By the definition of the sets,

$$P' \equiv a^{\phi(n)} P \pmod{n}.$$

However, we also concluded that the elements in the sets were the same modulo n, so

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

□

Since $\phi(p) = p - 1$ for a prime p, Euler's theorem completely generalizes Fermat's Little Theorem.

This was mentioned in the introductory lecture, but there are sometimes smaller cycles that exist within a cycle of length $\phi(n)$.

Definition 3.8. The order of an integer a in modulo n is defined as

$$\text{ord}_n(a) = k$$

where k is the smallest positive integer such that $a^k \equiv 1 \pmod{n}$.

The following result seems very straightforward, but requires a rigorous proof. We will use a **Proof by Contradiction**, where we assume the contrary and the prove that there exists a contradiction somewhere.

Theorem 3.9
For coprime integers a, n, $\text{ord}_n(a) \mid \phi(n)$.

Proof. Assume the contrary: there is a positive integer $k < \text{ord}_n(a)$ such that

$$\phi(b) \equiv k \pmod{\text{ord}_n(a)}.$$

Then, by definition of congruences, we can write

$$\phi(b) = m \cdot \text{ord}_n(a) + k$$

for some integer m. We can substitute this into Euler's theorem to conclude that

$$a^{\phi(n)} \equiv \left(a^{\text{ord}_n(a)}\right)^m \cdot a^k \equiv a^k \equiv 1 \pmod{n}.$$

However, this implies there is a positive integer $k < \text{ord}_n(a)$ where this statement is true, which contradicts the definition of order being the smallest. □

These types of proofs aren't uncommon at all, and given terms or conditions involving minimality or maximality, it may be intuitive to set up a contradiction.

Furthermore, order is sometimes helpful in occasional problems.

Example 3.10 (2019 AIME 1)
Find the least odd prime factor of $2019^8 + 1$.

Solution. Assume a prime p divides the expression. Thus, $2019^8 \equiv -1 \pmod{p}$. Squaring both sides gives $2019^{16} \equiv 1 \pmod{16}$. Since $16 = k$ satisfies $2019^k \equiv 1 \pmod{p}$ while no other divisors of 16 satisfy it, we know that $\text{ord}_p(2019) = 16$. By Theorem 3.9, we know that 16 divides $\phi(p) = p - 1$. The smallest prime which satisfies this is 17, but checking $2019^8 \equiv -1 \pmod{p}$ shows that 17 does not work. The next prime is 97, and checking this quickly shows that $\boxed{97}$ works. □

§4 Quadratic Congruences

In this section, we will introduce some basic information regarding the solutions to the congruence equation

$$x^2 \equiv a \pmod{n}.$$

Although it may not seem like it at first, this section is very connected to the previous section on exponents. To begin, we will define a crucial term for our study.

Definition 4.1. An integer a is a quadratic residue modulo n iff there exists an integer x such that $x^2 \equiv a \pmod{n}$. If no integer x exists, then a is quadratic non-residue.

Next, we will discuss another concept which is widely used not only for quadratic congruences.

§4.1 Generators

Definition 4.2. A generator ζ modulo n is an integer in which for every integer a coprime to n, there exists an integer k such that $\zeta^k \equiv a \pmod{n}$.

Essentially, ζ is able to "generate" all the numbers coprime to n. Generators are also oftentimes referred to as **Primitive Roots Modulo** n. Note that the generator is also coprime to n.

Theorem 4.3

An integer ζ is a generator if and only if $\text{ord}_n(\zeta) = \phi(n)$.

Proof. If ζ is a generator, it must produce $\phi(n)$ distinct values through exponentiation. By Euler's theorem, ζ cycles after $\phi(n)$; thus, $\text{ord}_n(\zeta) = \phi(n)$ in order to ensure that all $\phi(n)$ numbers are generated. The converse is obvious as no cycles implies that all numbers produced are unique; if they were not, then a cycle smaller than $\phi(n)$ exists. □

From here on out, we will be focusing primarily on modulo p for odd primes. It is here that quadratic residues are the most interesting. For primes, $\phi(p-1)$ generators exists. This can be proven with the identity involving a sum of totient functions.

Theorem 4.4

A generator ζ is a quadratic non-residue modulo p.

Proof. Assume the contrary: there exists an integer x such that $x^2 \equiv \zeta \pmod{p}$. Since p is an odd prime, there is an integer $k = (p-1)/2$. If we raise our quadratic congruence to the kth power, we have

$$\zeta^k \equiv x^{2k} \equiv x^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem. However, by Theorem 4.3, $\text{ord}_p(\zeta) = p - 1 > k = (p-1)/2$ which is a contradiction. □

Theorem 4.5

There exists exactly $(p-1)/2$ nonzero distinct quadratic residues modulo p and exactly $(p-1)/2$ quadratic non-residues between 1 and $p-1$.

Proof. Let ζ be a generator. Then, any even power of ζ is a residue. However, all odd powers are non-residues: if $\zeta^{2k+1} \equiv x^2 \pmod{p}$, then $x^2(\zeta^{-1})^{2k} \equiv \zeta \pmod{p}$ is a residue too, which contradicts Theorem 4.4. Thus, since there are an even $p-1$ integers from 1 to $p-1$, exactly half are residues and half are non-residues. □

§4.2 Legendre Symbol

We will introduce some notation which will be useful for determining residues.

Definition 4.6. We define the **Legendre Symbol** as

$$\left(\frac{a}{n}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } n \\ 0 & \text{if } a \equiv 0 \pmod{n} \\ -1 & \text{if } n \text{ is a quadratic non-residue} \end{cases}$$

The following properties are derived from the definition of residues.

Theorem 4.7

The Legendre Symbol has the properties for prime p:
(i) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
(ii) If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

It turns out that there is a closed form for the Legendre Symbol, although it is not very pleasant for calculations by hand.

Theorem 4.8

For integer a and odd prime p, we have the relation for $m = (p-1)/2$:

$$\left(\frac{a}{p}\right) \equiv a^m \pmod{p}.$$

Proof. We will prove this for each of the 3 cases in the Legendre Symbol.
Case 1: If a is a quadratic residue where $a \equiv x^2 \pmod{p}$, then $a^m \equiv x^{p-1} \equiv 1 \pmod{p}$ by Fermat's Little Theorem.
Case 2: If $p \mid a$, $a^m \equiv 0 \pmod{p}$.
Case 3: If a is a non-residue, then we can use generators. Let $a \equiv \zeta^k \pmod{p}$ for a generator ζ and integer k. Then $a^m \equiv \zeta^{km} \pmod{p}$ but k must be odd since a is not a quadratic residue as shown in Theorem 4.5. Thus, $\zeta km \equiv \zeta^k \pmod{p}$ and since $\text{ord}_p(\zeta) = p-1$ by Theorem 4.2, $\zeta^k \equiv -1 \pmod{p}$. □

The -1 can be shown to be the only possible value due to Theorem 4.4.
This theorem can be used to derive the following fact:

Theorem 4.9

For an odd prime p, we have

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4} \\ -1 & \text{if } p \equiv 3 \pmod{4} \end{cases}$$

Although its uses may seem limited, it can be used to demonstrate a much more useful theorem in mathematics.

Theorem 4.10

If p is an odd prime, and $p \mid x^2 + y^2$ for some integers x, y, then $p \equiv 1 \pmod{4}$.

Proof. If $p \mid x^2 + y^2$, we have $x^2 \equiv -y^2 \pmod{p}$ which implies

$$\left(\frac{x^2}{p}\right) = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{y^2}{p}\right)$$

by Theorem 4.6. Since x^2 and y^2 are quadratic residues, their Legendre symbols are 1; thus, $\left(\frac{-1}{p}\right) = 1$. By Theorem 4.9, we have that $p \equiv 1 \pmod{4}$. □

The following theorem will be the last one in this handout. Its proof is very rigorous and complex, and too long to fit into a single lesson. However, it is often useful when dealing with Legendre symbols, which sparingly appear in competitions.

Theorem 4.11 (Gauss's Law of Quadratic Reciprocity)
For odd primes p, q, we have the relation

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

It is said that Gauss discovered the proof when he was 19 years old. One of the many proofs in existence uses an expression known as a Gauss sum. Another proof uses lattices.

For computation, quadratic reciprocity can often be used to easily calculate Legendre symbols with larger numbers and primes.

Example 4.12
Evaluate $\left(\frac{37}{83}\right)$.

Solution. Using quadratic reciprocity, we can see that

$$\left(\frac{37}{83}\right)\left(\frac{83}{37}\right) = (-1)^{18\cdot 41} = 1.$$

Furthermore, using Theorem 4.7, $\left(\frac{83}{37}\right) = \left(\frac{9}{37}\right) = 1$ since 9 is a square. Thus, $\left(\frac{37}{83}\right) = \boxed{1}$. □

To conclude, some of the main strategies this handout would like to communicate include looking at sets of numbers and pairing special pairs, or looking through sequences or cycles inside sets. Oftentimes, learning and doing many proofs will result in better intuition that can help you understand how to approach a problem efficiently.

§5 Problems

Problem 5.1. Prove that within the first $10^8 + 1$ Fibonacci numbers, there exists a number ending in 4 zeros.

Problem 5.2. Prove that for an integer $n > 1$, $n \nmid 2^n - 1$.

Problem 5.3. For two coprime integers a, b, show that there exists integers m, n such that $a^m + b^n \equiv 1 \pmod{ab}$. Hint: Look for a system of congruences.

Problem 5.4 (1989 AIME)**.** 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.

Problem 5.5. Prove that there are infinitely many primes of the form $4k+1$ and $4k+3$.

Problem 5.6. For what primes p does there exist a solution for $x^2 \equiv -3 \pmod{p}$?

Problem 5.7 (1969 Putnam)**.** The positive integer n is divisible by 24. Show that the sum of all the positive divisors of $n-1$ (including 1 and $n-1$) is also divisible by 24.

Problem 5.8 (2011 USAJMO)**.** Find, with proof, all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.

§6 Further Reading

From my perspective as an author, this handout could be better, but is decent. However, much of the information pulled into this writing was from my own years of experience and learning from many different resources. It has been quite a long time since I was deeply fascinated by number theory, and I definitely cannot find every single material I used back then. However, I will list a couple links I have found with decent coverage and simplicity. You can always search on your own with keywords such as "number theory", "textbook", "pdf", etc.

https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2013/05/An-Introductory-in-Elementary-Number-Theory.pdf

https://napocaro.files.wordpress.com/2015/02/david_m-_burton_elementary_number_theory_sixth_bookfi-org.pdf

There is a distinction between elementary number theory and analytic number theory; the latter involves calculus techniques and is much more algebraic in nature. If you're well-versed in calculus, you can learn more from Apostol's Introduction to Analytic Number Theory.

Many problems I used were from this document, you can check it out if you want a better variety of practice:

https://artofproblemsolving.com/articles/files/SatoNT.pdf

If you'd like more of my own writing, you can contact me (Kevin Chang).