Lesson 12: Modular Arithmetic

Adithya B., Brian L., William W., Daniel X.

September 2020

Chinese Remainder Theorem

- The *Chinese Remainder Theorem* allows us to collate several congruences into a single congruence.
- Suppose $a_1, a_2, \ldots, a_n$ are pairwise coprime positive integers (so no two share any common factor greater than 1)
- Let $b_1, b_2, \ldots, b_n$ be arbitrary integers, and consider the system of congruences

$$x \equiv b_1 \pmod{a_1}, x \equiv b_2 \pmod{a_2}, \ldots, x \equiv b_n \pmod{a_n}$$

- Then this system of congruences is equivalent to the single congruence $x \equiv k \pmod{a_1 a_2 \cdots a_n}$ for some integer k
- In other words: if we know the residue of x modulo a_1, a_2, $\ldots$, a_n, then there is only one possible value for the residue of x modulo $a_1 a_2 \ldots a_n$
- Note that the theorem doesn't tell us what k is; it only tells us that it exists

Chinese Remainder Theorem

2012 AIME II #12

For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $\{3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, \ldots\}$. Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe, and 13-safe.

- When is n 7-safe?
- This happens when $n \equiv 3, 4 \pmod 7$
- When is n 11-safe?
- This happens when $n \equiv 3, 4, 5, 6, 7, 8 \pmod{11}$
- n is 13-safe if and only if $n \equiv 3, 4, 5, 6, 7, 8, 9, 10 \pmod{13}$

2012 AIME II # 12

- When is n 7-safe, 11-safe, and 13-safe?
- Since $\gcd(7, 11, 13) = 1$ we can use the Chinese Remainder Theorem
- If we pick the residues of n modulo 7, 11, and 13, we get a unique residue modulo $7 \cdot 11 \cdot 13 = 1001$
- We have 2 ways to choose modulo 7, 6 ways to choose modulo 11, and 8 ways to choose modulo 13
- $2 \cdot 6 \cdot 8 = 96$ residues modulo 1001 work
- Now want the number of $1 \leq n \leq 10000$ that work
- We know that $10 \cdot 96$ numbers in $1, 2, \ldots, 10 \cdot 1001$ work
- Now need to subtract working n in $10001, \ldots, 10010$ from total of 960
- Which of $10001, \ldots, 10010$ work?
- 10006 and 10007 (check this using that 10010 is divisible by 7, 11, 13)
- So $960 - 2 = \boxed{958}$

Chinese Remainder Theorem

2011 AIME II #14

There are N permutations $(a_1, a_2, \ldots, a_{30})$ of $1, 2, \ldots, 30$ such that for $m \in \{2, 3, 5\}$, m divides $a_{n+m} - a_n$ for all integers n with $1 \leq n < n + m \leq 30$. Find the remainder when N is divided by 1000.

- We get three choices for m; let's try $m = 2$ first
- Condition equivalent to $a_{n+m} \equiv a_n \pmod{m}$
- For $m = 2$ we find $a_1 \equiv a_3 \equiv \cdots \equiv a_{29}$, $a_2 \equiv a_4 \equiv \cdots \equiv a_{30} \pmod{2}$
- $a_1, a_2, \ldots, a_{30}$ permutation of $1, 2, \ldots, 30$, so 15 are odd and 15 are even
- 2 ways to choose residues modulo 2
- Let's move on to $m = 3$:

  $a_1 \equiv a_4 \equiv \cdots \equiv a_{28}$, $a_2 \equiv a_5 \equiv \cdots \equiv a_{29}$, $a_3 \equiv a_6 \equiv \cdots \equiv a_{30} \pmod{3}$

2011 AIME II # 14

- 10 of the a_i must be congruent to each of $0, 1, 2 \pmod 3$ since they're a permutation of $(1, 2 \ldots, 30)$
- 3! ways to choose residues modulo 3
- $m = 5$: $a_1 \equiv a_6 \equiv \cdots \equiv a_{26}, \ldots, \ a_5 \equiv a_{10} \equiv \cdots \equiv a_{30} \pmod 5$
- Same logic: 6 of the a_i congruent to each of $0, 1, 2, 3, 4 \pmod 5$, 5! ways to choose residues modulo 5
- Suppose we've chosen residues for a_i modulo 2, 3, and 5: then by CRT we've chosen a_i modulo 30
- Since $1 \leq a_i \leq 30$, a_i is uniquely defined
- But the sequence $a_1, \ldots, a_{30}$ needs to be a *permutation*: no two terms equal
- Suppose $a_i = a_j$
- Then $i \equiv j \pmod 2$, since:
- $a_1 \equiv a_3 \equiv \cdots \equiv a_{29} \not\equiv a_2 \equiv a_4 \equiv \cdots \equiv a_{30} \pmod 2$

2011 AIME II # 14

- Similarly $i \equiv j \pmod 3$, $i \equiv j \pmod 5$
- By CRT $i \equiv j \pmod{30}$
- Since $1 \leq i, j \leq 30$ this gives $i = j$
- So $a_i = a_j \implies i = j$ so $a_1, \ldots, a_{30}$ is guaranteed to be a permutation
- 2! ways to choose modulo 2, 3! ways modulo 3, 5! ways modulo 5
- Total $2! \cdot 3! \cdot 5! = 2 \cdot 6 \cdot 120 = 1440$
- $\boxed{440}$

Euler's Totient Theorem

- Define the totient of n, $\phi(n)$, to be the number of positive integers less than n that are relatively prime to n.
- If n has distinct prime factors $p_1, p_2, \ldots, p_k$,

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

- Probability that an integer is not divisible by p_1 is $1 - \frac{1}{p_1}$
- Multiply all the probabilities together and the number of positive integers (n), to get the value of $\phi(n)$.

Theorem (Euler's Totient)

Given an integer $n > 1$ and a natural a relatively prime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$

Euler's Totient Theorem

- Proof: S the set of residues mod n which are relatively prime with n.
- Consider the set $T = \{as \pmod{n} | s \in S\}$
- We claim the elements in S are the same as the elements in T.
- To show this, we will first show that this is an injective map; that is, for distinct $s, s' \in S$, $as \not\equiv as' \pmod{n}$.
- Suppose $as \equiv as' \pmod{n}$ for $s \not\equiv s'$. Since, $\gcd(a, n) = 1$, we can divide by a to get $s \equiv s' \pmod{n}$, a contradiction.
- This means $|S| = |T|$ because every element in S maps to a distinct element in T.
- All the elements of T are relatively prime with n, so $S = T$
- Thus, the products of the elements in S and T are the same.

$$\prod_{s \in S} s \equiv \prod_{t \in T} t \pmod{n} \implies \prod_{s \in S} s \equiv \prod_{s \in S} as \equiv a^{\phi(n)} \prod_{s \in S} s \pmod{n}$$

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

Fermat's Little Theorem

Fermat's Little Theorem

For any prime p and positive integer a coprime to p, we have $a^{p-1} \equiv 1 \pmod{p}$

Proof.

This is just Euler's Totient Theorem at $n = p$. □

Fermat's Little Theorem

NIMO

Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p.

- How do we start?
- Let's get rid of the floors!
- From FLT, we note $a^p \equiv a \pmod{p}$, so $\left\lfloor \frac{a^p}{p} \right\rfloor = \frac{a^p - a}{p}$.
- Our sum becomes $\sum_{a=1}^{p-2} \frac{a^p - a}{p} \pmod{p}$.
- It suffices to find $\sum_{a=1}^{p-2} (a^p - a) \pmod{p^2}$.
- How can we evaluate this sum?

- Euler's Totient in $\bmod p^2$ doesn't appear to be helpful.
- Let's try pairing the terms in the sum.

$$\begin{aligned} a^p + (p-a)^p &= a^p + p^p - \binom{p}{p-1} p^{p-1} a + \cdots + \binom{p}{1} p a^{p-1} - a^p \\ &= p^p - \binom{p}{p-1} p^{p-1} a + \cdots + \binom{p}{1} p a^{p-1} \\ &\equiv 0 \pmod{p^2} \end{aligned}$$

- $(a^p - a) + ((p-a)^p - p + a) \equiv 0 - p \equiv -p \pmod{p^2}$.
- How many pairs do we have?
- $\sum_{a=1}^{p-2} (a^p - a) \equiv \frac{p-3}{2} \cdot (-p) = -\frac{p(p-3)}{2} \equiv \frac{p(p+3)}{2} \pmod{p^2}$
- $\sum_{a=1}^{p-2} \frac{a^p - a}{p} \equiv \frac{\frac{p(p+3)}{2}}{p} \equiv \frac{p+3}{2} \pmod{p}$
- $p = 2017$, so we get $\boxed{1010}$.

Fermat's Little Theorem

Bulgaria 1996

Find all pairs of primes p, q such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

- Equation is symmetric; WLOG, assume $p \geq q$.
- By Fermat's Little Theorem,

$$5^p - 2^p \equiv 3 \pmod{p}$$

$$5^q - 2^q \equiv 3 \pmod{q}$$

- $q = 2$ doesn't work.
- If $q = 3$, we have $q \mid (5^q - 2^q)$. What values of p work?
- $p = 3$ works because then $p \mid (5^p - 2^p)$.
- If $p > 3$, then $p \nmid (5^p - 2^p)$, so $p \mid (5^q - 2^q) = 117$. Thus, $p = 13$.
- Solutions so far are $(3, 3), (3, 13), (13, 3)$ (accounting for permutations).
- Now, assume $p \geq q > 3$.

Bulgaria 1996

- We must have $q \mid (5^p - 2^p)$. This means $5^p \equiv 2^p \pmod{q}$.
- From FLT, $5^{q-1} \equiv 2^{q-1} \equiv 1 \pmod{q}$.
- Can we combine these two expressions somehow?
- Since $\gcd(p, q-1) = 1$, there exist integers a, b such that $ap + b(q-1) = \gcd(p, q-1) = 1$.

$$5^{ap+b(q-1)} = (5^p)^a \cdot (5^{q-1})^b = (2^p)^a \cdot (2^{q-1})^b = 2^{ap+b(q-1)} \pmod{q}.$$

- Since $ap + b(q-1) = 1$, we get $5 \equiv 2 \pmod{q}$, a contradiction to $q > 3$.
- Our only solutions are $\boxed{(3,3), (3,13), (13,3)}$.

Orders

- From Fermat's Little Theorem, we know $a^{p-1} \equiv 1 \pmod{p}$, but do we always need to raise a to such a high power to get 1?
- For example, FLT tells us that $2^6 \equiv 1 \pmod{7}$, but in fact 2^3 works as well
- Motivated by this question, we define the *order* of $a \pmod{p}$ to be the minimum exponent e such that $2^e \equiv 1 \pmod{p}$. e will be denoted as $\text{ord}_p(a)$
- Order exists since it is at most $p - 1$
- Let's prove some properties!

Orders

Order divisibility

If $a^k \equiv 1 \pmod{p}$ for prime p and $p \nmid a$, then $\text{ord}_p(a) | k$.

- Denote e as $\text{ord}_p(a)$. Which r satisfy $a^r \equiv 1$?
- All multiples of e do. Choose a convenient one.
- Consider a^{ne} where $ne \leq k < (n+1)e$. Then, we know

$$a^{ne} \equiv a^k \equiv 1 \pmod{p}$$

What can we say now?

- $a^{k-ne} \equiv 1 \pmod{p}$. Why is this good?
- $k - ne < e$, so by minimality $k = ne$, as desired. $\square$
- As a corollary, this tells us that $e | p - 1$.

Primitive Roots

- Now that we have orders, it is natural to ask if Fermat's Little Theorem is tight. Namely, do there exist a with order equal to $p-1$?
- The answer is actually yes for all primes. Such a are known as *primitive roots*

Existence of Primitive Roots

Gauss

For any prime p, there exists a residue with order $p-1$.

- Before we prove this result, we begin with a lemma:

Lagrange

A polynomial $P(x)$ has at most $\deg P$ roots modulo p.

- Why is this lemma true in reals? Can we try something similar?
- We will try to factor $P(x)$. Consider a root of $P(x)$, r. What happens when we divide $P(x)$ by $x-r$?
- Division algorithm still works mod p, so we get $P(x) \equiv Q(x)(x-r)+c$. What should c be?
- r is a root, so by definition $P(x) \equiv (x-r)Q(x) \pmod{p}$ for some Q.
- Finish by induction

Existence of Primitive Roots

- Now, we will show that $x^k - 1$ actually has **exactly** k roots when $k|p-1$
- Note that our lemma is tight at $x^{p-1} - 1$, since this polynomial has $p-1$ roots. What happens when we factor it as

$$x^{p-1} - 1 = (x^k - 1)Q(x)$$

- How many roots does the RHS have?
- The RHS has at most $k + (p - 1 - k) = p - 1$ roots, so in order for this to be true, equality must hold for both $x^k - 1$ and $Q(x)$. So, $x^k - 1$ has k roots
- Now, denote $N(e)$ to be the number of residues with order e, for all $e|p-1$. What can we say about the sum of all $N(e)$?

Existence of Primitive Roots

- $\sum_{e|p-1} N(e) = p - 1$. Does this remind you of anything?
- What are the roots of $x^k - 1$?
- They are residues with orders which divide e. So,

$$\sum_{e|k} N(e) = k$$

- Using this relation with k at every divisor of $p - 1$, we can uniquely determine $N(e)$
- But we know $N(e) = \phi(e)$, so ϕ has to be our unique function!
- So, we have $N(p - 1) = \phi(p - 1) \geq 1$ primitive roots
- Note that this proof also tells us that there are exactly $\phi(e)$ residues with order e.

Order

2019 AIME I #14

Find the least odd prime factor of $2019^8 + 1$.

- Suppose p divides this number. What can we say about the order of 2019?
- $2019^8 \equiv -1 \pmod{p} \implies 2019^{16} \equiv 1 \pmod{p}$. So, $e|16$
- Can order be anything less than 16?
- No, since otherwise $2019^8 \equiv 1 \pmod{p}$. So, we have $e = 16$. What does this tell us about p?
- $16|p-1$. So, p is $1 \pmod{16}$. Now, we can just check primes of this form.
- Check $p = 17, 97$. We'll skip the details, but it is easy to verify that 17 doesn't work and 97 does, so our answer is $\boxed{97}$.

Order

HMMT 2016

For positive integers n, let c_n be the smallest positive integer for which $n^{c_n} - 1$ is divisible by 210, if such a positive integer exists, and $c_n = 0$ otherwise. What is $c_1 + c_2 + \cdots + c_{210}$?

- What is c_n?
- c_n is the "order" of n (mod 210). However, 210 is not prime. How can we fix this?
- If w_n, x_n, y_n, z_n are the orders of n modulos $2, 3, 5, 7$ respectively, what is c_n?
- $c_n = \text{lcm}(w_n, x_n, y_n, z_n)$
- We can consider w, x, y, z separately by Chinese Remainder Theorem. Let's look at z_n. What can z_n be?

- There are 6 different nonzero residues mod 7. Out of these, which ones have which order?
- We have 2 with order 6, 2 with order 3, 1 with order 2 and 1 with order 1
- Similarly, y_n is $(4, 2, 1)$ with frequencies $(2, 1, 1)$, x_n is $(2, 1)$ with frequencies $(1, 1)$, and w_n is always 1.
- From here, we can just do casework on the divisors of 12. However, we can be slightly cleverer by noticing that the powers of $3, 2$ dividing c_n are actually independent.
- What is the probability that c_n is divisible by 3?
- A power of 3 must come from z_n, which is divisible by 3 exactly $\frac{2}{3}$ of the time
- How often is c_n a multiple of 4? How often is it odd?

- c_n is a multiple of 4 when $y_n = 4$, which happens with probability $\frac{1}{2}$
- c_n is odd when $z_n = 1, 3$ and everything else is 1. This happens with probability $\frac{1}{2} \cdot \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{16}$
- So, the expected value of the power of 2 is

$$1 \cdot \frac{1}{16} + 2 \cdot \frac{7}{16} + 4 \cdot \frac{1}{2} = \frac{47}{16}$$

- Similarly, the expected value of the power of 3 is $1 \cdot \frac{1}{3} + 3 \cdot \frac{2}{3} = \frac{7}{3}$
- So, the expected value of a nonzero c is $\frac{47}{16} \cdot \frac{7}{3} = \frac{329}{48}$
- There are $\phi(210) = 48$ nonzero c, so our answer is $\frac{329}{48} \cdot 48 = \boxed{329}$

Order

HMMT 2014

Determine the sum of all positive integers m such that $1 \leq m \leq 50$ and there exists an integer n for which m divides $n^{n+1} + 1$.

- Are there any m which obviously work?
- If we naively set $n \equiv -1 \pmod{m}$, as long as $n+1$ is odd this will work. Hence, $n = m - 1$ works for all odd m
- For even m, we will first introduce a lemma:

Weak Fermat's Christmas Theorem

Any odd prime which divides $x^2 + y^2$ but not x, y must be $1 \pmod{4}$

- Writing in terms of mods, $x^2 \equiv -y^2 \pmod{p}$
- This means that $\left(\frac{x}{y}\right)^2 \equiv -1 \pmod{p}$

- This means that the order of x/y is 4. What does this tell us about p?
- $4|p-1$ so $p \equiv 1 \pmod 4$, as desired. $\square$
- Going back to the question at hand, m is even means that n must be odd. What does this tell us about n^{n+1}?
- $n+1$ is even so n^{n+1} is a square! So, by our lemma, if $m|n^{n+1}+1$, then any odd prime dividing m must be $1 \pmod 4$
- Furthermore, $n^{n+1}+1 \equiv 2 \pmod 4$, so m cannot be divisible by 4. What does this give us for the set of possible even m?
- Primes under 25 which are $1 \pmod 4$ are $5, 13, 17$, so we can only have $m = 2, 10, 26, 34, 50$. Do these all work?
- To construct, we need n such that $n^{n+1} = (n^2)^{(n+1)/2} \equiv -1 \pmod m$
- So, let's choose n such that $n^2 \equiv -1 \pmod m$ and $(n+1)/2$ is odd. Is this always possible?

- First, $(n+1)/2$ is odd when $n \equiv 1 \pmod 4$. What about the first condition?
- We are actually guaranteed such an n by Fermat's Christmas Theorem, but since there are so few candidates for m, we can just bash.
- For $m = 2, 10, 26, 34, 50$ choose $n = 1, 3, 5, 13, 7$ in the respective mods. Now, just choose suitable n for each of the cases by Chinese Remainder Theorem.
- Hence, the sum of all possible m is

$$(1 + 3 + 5 + \ldots + 49) + (2 + 10 + 26 + 34 + 50) = \boxed{747}$$

Order

Online Math Open 2013

Find the sum of all integers m with $1 \leq m \leq 300$ such that for any integer n with $n \geq 2$, if $2013m$ divides $n^n - 1$, then $2013m$ also divides $n - 1$.

- We let $M = 2013m$. We wish to characterize all such M.
- Suppose we let p^k be any prime divisor of M.
- Now, we have $\text{ord}_{p^k}(n) \mid n$ and we want $\text{ord}_{p^k}(n) = 1$
- We also have $\text{ord}_{p^k}(n) \mid p^{k-1}(p-1)$.
- If we had $\gcd(p^{k-1}(p-1), n) = 1$, that would be sufficient. We already have $\gcd(p, n) = 1$
- If we had $q \mid M$ for each $q \mid p - 1$, that would be sufficient, since we have $\gcd(M, n) = 1$.
- We now will prove that this is necessary.
- Suppose $p^k \mid M, q \mid p - 1, q \nmid M$.
- We now will construct an n such that $M \mid n^n - 1$ and $M \nmid n - 1$.

Online Math Open 2013

- We first let $n \equiv 1 \pmod{\frac{M}{p^k}}$.
- Now, we want to find an a such that $a \not\equiv 1 \pmod{p^k}$ while $a^q \equiv 1 \pmod{p^k}$.
- Let g be a primitive root mod$p$. We note that $a = g^{p^{k-1}\frac{p-1}{q}}$ works.
- Now, let $n \equiv a \pmod{p^k}$ and $n \equiv 0 \pmod{q}$, and this is sufficient to construct a counterexample, as desired.
- Thus, our condition is necessary.
- Now, note that $2013 = 3 \cdot 11 \cdot 61$.
- Now, we have $2, 5 \mid 11 - 1$, so we need $10 \mid M$.
- Now, we test all multiple of 10 as values of m.
- Note that all of them work except $m = 290$, since in that case, we'd need $7 \mid M$, which is false.
- Thus, we have our answer is $10(\frac{30 \cdot 31}{2}) - 290 = \boxed{4360}$.

Order

China 2009

Find all pairs of primes p, q such that $pq \mid 5^p + 5^q$.

- We split into cases. First, what if we had $p = q$?
- We get $p^2 \mid 2 \cdot 5^p$
- Thus, we get $p = 5$.
- Now, suppose $p \neq q$.
- Now, what if $q = 5$?
- We find $p \mid 5^p + 5^5$.
- We have $5^p \equiv 5 \pmod{p}$, so $p \mid 5^5 + 5$.
- We find $p \mid 3130$, so $p = 2, 313$, so we have the solutions $(2, 5), (5, 2), (313, 5), (5, 313)$.
- Now, what if neither of p, q were 5.
- What if $q = 2$.
- We have $p \mid 5^p + 5^2$, so $p \mid 5^2 + 5$, so $p = 3$.
- Now, we have the pairs $(2, 3), (3, 2)$.

China 2009

- Now, we consider the case where p, q are distinct primes not equal to $2, 5$.
- Now, suppose we have $p \mid 5^p + 5^q$.
- Then, we have $p \mid 5^{q-1} + 1$
- Now, suppose we defined $\nu_2(n)$ to be the largest k such that $2^k \mid n$.
- We find $\nu_2(\text{ord}_p(5)) = \nu_2(2(q-1)) \leq \nu_2(p-1)$.
- Similarly, $\nu_2(2(p-1)) \leq \nu_2(q-1)$
- This is a contradiction, since we get $\nu_2(p-1) \geq \nu_2(p-1) + 2$.
- Thus, we find our solutions are $\boxed{(5,5), (2,5), (5,2), (5,313), (313,5), (2,3), (3,2)}$.