Modular Arithmetic

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

9/2

§1 Chinese Remainder Theorem

Oftentimes, we need to handle congruences modulo composite numbers, e.g. modulo 6, or modulo 210, etc. The *Chinese Remainder Theorem* is a useful tool that allows us to transfer from multiple congruences to a single congruence:

Theorem 1.1 (Chinese Remainder Theorem)

Let $a_1, a_2, \ldots, a_n$ be pairwise coprime positive integers (that is, no two of these numbers share a common factor greater than one), and $b_1, b_2, \ldots, b_n$ be any integers. Then the system of n congruences

$$\begin{aligned} x &\equiv b_1 \pmod{a_1}, \\ x &\equiv b_2 \pmod{a_2}, \\ &\cdots, \\ x &\equiv b_n \pmod{a_n} \end{aligned}$$

is equivalent to the congruence $x \equiv k \pmod{a_1 a_2 \cdots a_n}$ for some integer k. That is, x satisfies all n congruences above if and only if $x \equiv k \pmod{a_1 a_2 \cdots a_n}$.

Note that this is an *existence* theorem: it does not tell us how to find k. For example, the theorem tells us that

$$x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5},$$

is equivalent to $x \equiv k \pmod{30}$ for some integer k, but it does not tell us what k is. (We can manually find that $k = 23$.)

The Chinese Remainder Theorem is especially powerful because it allows us to collate multiple congruences into a single congruence without having to actually solve the system of congruences. This will be essential for the problems below.

Example 1.2 (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.

Solution. The p-safe condition translates nicely into modular arithmetic. In order for n to be 7-safe, it has to be more than two away from any multiple of 7. This means it has to be congruent to 3 or 4 modulo 7. Conversely, if n is congruent to 3 or 4 modulo 7 then it is more than 2 away from the nearest multiple of 7.

Similarly, n is 11-safe if and only if it is congruent to $3, 4, 5, 6, 7$, or 8 modulo 11, and n is 13-safe if and only if it is congruent to $3, 4, 5, 6, 7, 8, 9$, or 10 modulo 13. For n to be simultaneously 7-safe, 11-safe, and 13-safe, all of the following congruences must be satisfied:

- $n \equiv 3, 4 \pmod 7$,
- $n \equiv 3, 4, 5, 6, 7, 8 \pmod{11}$,
- $n \equiv 3, 4, 5, 6, 7, 8, 9, 10 \pmod{13}$.

Moreover, 7, 11, and 13 are pairwise relatively prime (they are all prime), so we can use the Chinese Remainder Theorem to splice together these conditions. For example, the congruences

- $n \equiv 4 \pmod 7$,
- $n \equiv 8 \pmod{11}$,
- $n \equiv 3 \pmod{13}$.

have a unique solution modulo $7 \cdot 11 \cdot 13 = 1001$. To find all possible solutions modulo 1001, we need to pick a residue modulo 7, a residue modulo 11, and a residue modulo 13; each such choice results in exactly one residue modulo 1001. With our list above, we find that this can be done in $2 \cdot 6 \cdot 8 = 96$ ways. So there are 96 residues modulo 1001 that are 7-safe, 11-safe, and 13-safe.

We now want to find the number of positive integers at most $10,000$ that work. From our work above, we see that:

- There are 96 working integers in $\{1, 2, \ldots, 1001\}$,
- There are 96 working integers in $\{1002, 1003, \ldots, 2002\}$,
- $\ldots$,
- There are 96 working integers in $\{9010, 9011, \ldots, 10010\}$.

So there are 960 working integers from 1 to 10010, inclusive. We just need to examine the integers $10001, \ldots, 10010$ and subtract any overcounts to find the final answer.

Note that 10010 is a multiple of 7, 11, and 13. The next smallest multiples of 7, 11, and 13 are 10003, 9999, and 9997, respectively. From this, we see that the only working integers from 10001 to 10010 are 10006 and 10007. So we have two overcounts, and the number of positive integers less than or equal to $10,000$ which are 7-safe, 11-safe, and 13-safe is $960 - 2 = \boxed{958}$. □

Example 1.3 (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.

Solution. We're given three different values of m to use; let's investigate them separately. For $m = 2$, the condition implies that

$$a_1 \equiv a_3 \equiv \cdots \equiv a_{29}, \ a_2 \equiv a_4 \equiv \cdots \equiv a_{30} \pmod 2$$

Since the a_i need to be a permutation of $(1, 2, \ldots, 30)$, with 15 odd numbers and 15 even numbers, this implies that $a_1, a_3, \ldots, a_{29}$ are all of the opposite parity as $a_2, a_4, \ldots, a_{30}$. Thus we can choose that either $a_1, a_3, \ldots, a_{29}$ are all even, or $a_1, a_3, \ldots, a_{29}$ are all odd. There are 2 ways to do this.

Let's take a look modulo 3. The condition gives us

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

Again, since the a_i are a permutation of $(1, 2, \ldots, 30)$, 10 of them congruent are to each of $0, 1$, and 2 modulo 3. So we can choose what $a_1, a_4, \ldots, a_{28}$ are modulo 3, then pick a different residue for $a_2, a_5, \ldots, a_{29}$, and use the last residue for $a_3, a_6, \ldots, a_{30}$. We have $3! = 6$ ways to do this.

Finally, for $m = 5$ we can use the same logic. We get

$$a_1 \equiv a_6 \equiv \cdots \equiv a_{26}, \ a_2 \equiv a_7 \equiv \cdots \equiv a_{27}, \ldots, \ a_5 \equiv a_{10} \equiv \cdots \equiv a_{30} \pmod 5.$$

We can choose the residues of $a_1, a_6, \ldots, a_{26}$ modulo 5, then pick a different residue for $a_2, a_7, \ldots, a_{27}$, and so on up to $a_5, a_{10}, \ldots, a_{30}$. There ae $5! = 120$ ways to assign residues modulo 5.

We have now chosen a residue for each a_i modulo $2, 3$, and 5; by the Chinese Remainder Theorem this results in a unique residue modulo 30, and hence a unique element of $\{1, 2, \ldots, 30\}$. So our choices uniquely define the sequence $(a_1, a_2, \ldots, a_{30})$. We're not done yet; we need to check if this sequence is a permutation. That is, we need to check that no two elements are equal.

What happens if $a_i = a_j$? This means that $a_i \equiv a_j \pmod 2$, so that $i \equiv j \pmod 2$. We see this because

$$a_1 \equiv a_3 \equiv \cdots \equiv a_{29} \not\equiv a_2 \equiv a_4 \equiv \cdots \equiv a_{30} \pmod 2.$$

Similarly, $a_i \equiv a_j \pmod 3$, so $i \equiv j \pmod 3$, and since $a_i \equiv a_j \pmod 5$ we have $i \equiv j \pmod 5$. By the Chinese Remainder Theorem, we have $i \equiv j \pmod{30}$. But i and j are between 1 and 30, so this forces $i = j$. Hence we conclude that our sequence is a permutation; no two terms are equal. We had 2! ways to set the residues modulo 2, 3! ways to set the residues modulo 3, and 5! ways to set the residues modulo 5, so the total number of ways is

$$2! \cdot 3! \cdot 5! = 2 \cdot 6 \cdot 120 = 1440$$

and the answer is $\boxed{440}$. □

§2 Euler's Totient Theorem

Euler's Totient Theorem is probably the most important theorem for dealing with exponents in modular arithmetic. Using it, one can compute the residue of large powers of numbers modulo a fixed n without having to resort to techniques such as "looking for patterns." To understand it, first we must know what the totient function is.

Definition 2.1. The *totient* of n, denoted $\phi(n)$, is the number of positive integers less than or equal to n which are relatively prime to it.

We won't go over it's proof in this class, but the totient is easily computable via the closed form

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

where $p_1, p_2, \ldots, p_k$ are the primes dividing n, listed without repetition. The proof can be done using Chinese Remainder Theorem on mods $p_1, \ldots, p_k$ and is left as an exercise to the reader.

Theorem 2.2 (Euler's Totient Theorem)
Given an integer $n > 1$ and a natural a relatively prime to n, we have $a^{\phi(n)} \equiv 1 \pmod{n}$

Proof. Denote S the set of residues mod$n$ which are coprime with n. By definition, $|S| = \phi(n)$. Now, consider the set $T = \{as \pmod{n} | s \in S\}$, which is the set of the residues multiplied by a. As a is coprime with n, all elements of T are coprime with n as well. Furthermore, no two elements in T are the same, since $as \equiv as' \pmod{n} \implies s \equiv s' \pmod{n}$. So, T is a set of numbers coprime to n with magnitude $|T| = |S| = \phi(n)$. Hence, $T = S$.

Of course, as they are the same set, the product of all the elements should be the same too. Hence,

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

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

as desired. □

Corollary 2.3
Fermat's Little Theorem For any prime p and a coprime to p, we have $a^{p-1} \equiv 1 \pmod{p}$

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

Example 2.4 (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.

Solution. First, let's try to get rid of the floors. From FLT, we note $a^p \equiv a \pmod{p}$, so

$$\left\lfloor \frac{a^p}{p} \right\rfloor = \frac{a^p - a}{p}.$$

Therefore, it suffices to determine

$$\sum_{a=1}^{p-2} \frac{a^p - a}{p} \pmod{p}$$

which is equivalent to finding $\sum_{a=1}^{p-2}(a^p - a) \pmod{p^2}$. It isn't immediately apparent how to find this. Euler's theorem would only be helpful if the exponent was close to $p(p-1)$. Therefore, we instead try another trick. Let's try to pair up terms in the sum by adding the terms for a and $p - a$. Note that

$$a^p + (p-a)^p = a^p + p^p - \binom{p}{p-1}p^{p-1}a + \cdots + \binom{p}{1}pa^{p-1} - a^p \equiv 0 \pmod{p^2}$$

since every remaining term in the sum is divisible by p^2 (The last term in the expansion of $(p-a)^p$ is negative because p is an odd prime). Now, we have

$$(a^p - a) + ((p-a)^p - p + a) \equiv 0 - p \equiv -p \pmod{p^2}.$$

Now, the first term in the sum $\sum_{a=1}^{p-2}(a^p - a) \pmod{p^2}$ is 0, and the other $p-3$ terms can be paired up so that the total value is

$$\sum_{a=1}^{p-2}(a^p - a) \equiv \frac{p-3}{2} \cdot (-p) = -\frac{p(p-3)}{2} \equiv \frac{p(p+3)}{2} \pmod{p^2}.$$

Therefore, we have

$$\sum_{a=1}^{p-2} \frac{a^p - a}{p} \equiv \frac{\frac{p(p+3)}{2}}{p} \equiv \frac{p+3}{2} \pmod{p}.$$

For $p = 2017$, the answer is $\boxed{1010}$. □

Example 2.5 (Bulgaria 1996)

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

Solution. WLOG, let's assume $p \geq q$. By Fermat's Little Theorem,

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

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

Now, if $q = 3$, then we see that we can also have $p = 3$. If $q = 3$ and $p > 3$, then $p|(5^3 - 2^3) = 117$. This implies $p = 13$. Therefore, with permutations, we obtain the pairs $(3, 3), (3, 13), (13, 3)$.

Now, let's assume $p \geq q > 3$. In this case, clearly $\gcd(q, 5^q - 2^q) = 1$, so $5^p - 2^p \equiv 0 \pmod{q}$. This implies $5^p \equiv 2^p \pmod{q}$. From FLT again, we know $5^{q-1} \equiv 2^{q-1} \equiv 1 \pmod{q}$. Now, since $\gcd(p, q-1) = 1$, there exist integers a, b such that

$$ap + b(q-1) = \gcd(p, q-1) = 1.$$

Note that

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

However, this implies $5 \equiv 2 \pmod{q}$, which can only happen when $q = 3$, so we are done. The only solutions are $\boxed{(3, 3), (3, 13), (13, 3)}$. □

§3 Orders

From Fermat's Little Theorem, we know that $a^{p-1} \equiv 1 \pmod{p}$ for $p \nmid a$. But, often times we don't need to raise a to that high of a power in order to get it to $1 \pmod{p}$. For example, $2^6 \equiv 1 \pmod{7}$, but $2^3 \equiv 1$ as well.

This motivates us to define the order of $a \pmod{p}$, which is the minimum $e > 0$ such that $a^e \equiv 1 \pmod{p}$, denoted $e = \text{ord}_p(a)$. Note that order exists, since it is at most $p - 1$.

Theorem 3.1

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

Proof. Denote $e = \text{ord}_p(a)$. By definition, $a^e \equiv 1 \pmod{p}$, so $a^{ne} \equiv 1 \pmod{p}$ for any n by raising both sides to the nth power. So, choose n such that $ne \leq k < (n+1)e$. This way, by dividing the relations, we get $a^r \equiv 1 \pmod{p}$, where $r = k - ne$ is the remainder when k is divided by e.

However, $0 \leq r < e$, and e was defined to be the minimal positive power of a to yield $1 \pmod{p}$. Hence, we must have $r = 0$ and $e|k$, as desired. □

Corollary 3.2

$\text{ord}_p(a)$ divides $p - 1$

Proof. We know $a^{p-1} \equiv 1 \pmod{p}$, and applying Theorem 3.1 gives the desired result. □

As orders can be really small, a natural follow-up question might be whether or not FLT is actually tight. In fact, there do exist numbers with order $p - 1$ for all primes p, and such numbers are known as primitive roots.

Theorem 3.3 (Gauss)

Every prime admits a primitive root.

Proof. We first begin with Lagrange's Theorem which is obviously true for the reals but also holds mod p:

Theorem 3.4 (Lagrange)
A polynomial $P(x)$ has at most $\deg P$ roots modulo p.

Proof. We prove this with induction on $\deg P$. The result is clear when $\deg P = 1$. Now, suppose that we have the claim for polynomials of degree $\deg P - 1$.

If P does not have any roots modulo p, then we are already done. Otherwise, suppose it has root r. We can perform synthetic division on P to get $P(x) \equiv (x-r)Q(x)+k \pmod{p}$. However, since r is a root, $k = 0$. So, $P(x) \equiv (x-r)Q(x) \pmod{p}$. Now, $Q(x)$ has degree 1 less than P, so it has at most $\deg P - 1$ roots. Hence, P has at most $\deg P$ roots. □

Now, note that if $k|p-1$ for some k, then we can write

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

for some Q. $x^{p-1}-1$ admits $p-1$ roots by FLT, so the RHS should also have $p-1$ roots. However, $x^k - 1$ has at most k roots and $Q(x)$ has at most $p-1-k$, by Lagrange's Theorem. So, in order for equality to hold, $x^k - 1$ actually has exactly k roots.

Now, we are ready to finish. Let $N(e)$ denote the number of residues modulo p with order e. By Theorem 3.1, we have that

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

for any $k|p-1$, since the residues which satisfy $x^k \equiv 1$ are precisely those whose orders divide k. However, we've seen this type of summation a long time ago, we can compute $N(e)$ explicitly with Mobius Inversion! In fact, we get that

$$N(e) = \sum_{i|e} i\mu\left(\frac{e}{i}\right) = \phi(e)$$

(if you are unfamiliar with Mobius Inversion, you can also note that the function $N(e)$ is uniquely defined by the summation relation, and $\phi(e)$ works by Dirichlet Convolution, so it has to be the correct function.)

As $N(p-1)$ denotes the number of primitive roots, we see that we actually have $\phi(p-1)$ primitive roots $\pmod{p}$, as desired. □

Remark 3.5. The existence of a primitive root actually allows us to "generate" all elements of the residue class. To see this, let ζ be a primitive root modulo p. Since $\zeta^k \neq 1 \pmod{p}$ for any $k < p-1$, this means that the sequence $\zeta, \zeta^2, \ldots, \zeta^{p-1}$ does not cycle, and hence must cover every single nonzero residue.

In fact, if we can express a number a as $\zeta^k \pmod{p}$, this gives us a very efficient way to compute its order. We have that $a^e \equiv \zeta^{ke}$, and the order of ζ is known to be $p-1$. Hence,

$$a^e \equiv 1 \pmod{p} \iff p-1|ke \iff \frac{p-1}{\gcd(k,p-1)}\Big|e$$

Hence, the order of a is $\frac{p-1}{\gcd(k,p-1)}$. Using ζ as a generator, see if you can rederive the fact that $N(e) = \phi(e)$.

Example 3.6 (2019 AIME I #14)
Find the least odd prime factor of $2019^8 + 1$.

Solution. If $p \mid 2019^8 + 1$, then $2019^8 \equiv -1 \pmod{p}$. Therefore, $2019^{16} \equiv (-1)^2 = 1 \pmod{p}$. Since $2019^8 \not\equiv 1 \pmod{p}$ and $2019^{16} \equiv 1 \pmod{p}$, we have that $\text{ord}_p(2019) = 16$. Since $\text{ord}_p(2019) \mid p-1$, we have $16 \mid p-1$. This implies $p \equiv 1 \pmod{16}$. We can now test primes to find the smallest odd prime that divides $2019^8 + 1$. The first few primes that are 1 mod 16 are 17 and 97. Note that

$$2019^8 \equiv (-4)^8 \equiv 16^4 \equiv (-1)^4 \equiv 1 \pmod{17}$$

so 17 does not divide it. Also, note that

$$2019^8 \equiv (-18)^8 \equiv 33^4 \equiv 22^2 = 484 \equiv -1 \pmod{97}.$$

Therefore, the smallest odd prime factor is $\boxed{097}$. □

Example 3.7 (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 $c_1 + c_2 + \cdots + c_{210}$?

Solution. Note that c_n is basically just the "order" of c_n mod 210.. Unfortunately, many of the theorems we have proven above only apply to primes. So, in order to compute c_n, we instead consider the orders of n mods $2, 3, 5, 7$. If we denote them as w_n, x_n, y_n, z_n respectively, then we have that $c_n = \text{lcm}(w_n, x_n, y_n, z_n)$.

However, we already have a good idea about the distributions of w_n, x_n, y_n, z_n by our proof of Theorem 3.3. This is because we know exactly $\phi(k)$ of the $p-1$ residues mod p have order k, where $k|p-1$.

Let's see how this applies to z_n, for example. 7 has 6 nonzero residues, and by the above we know 2 of them have order 6, 2 have order 3, 1 has order 2 and 1 has order 1. So, the orders $(1, 2, 3, 6)$ occur in ratio $1 : 1 : 2 : 2$.

Similarly, $y_n = (1, 2, 4)$ occurs in ratio $1 : 1 : 2$, $x_n = (1, 2)$ occurs in ratio $1 : 1$, and w_n is always 1.

Now, note that the lcm of all possible values of w_n, x_n, y_n, z_n is 12, so $c|12$. Now, it suffices to find out how often each divisor of 12 occurs.

The only way $4|c_n$ is if $y_n = 4$, which has probability $\frac{1}{2}$, and the only way it is not divisible by 2 is if $z_n = 1, 3$, and everything else is 1, which happens with probability $\frac{1}{2} \cdot \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{16}$. Hence, c_n has a $\frac{1}{16}$ chance of being odd, $\frac{7}{16}$ chance of being divisible by 2 but not 4, and a $\frac{1}{2}$ chance of being divisible by 4.

On the other hand, factors of 3 only come from z_n. It's easy to see that it has probability $\frac{2}{3}$ of being divisible by 3. Now, as the powers of $2, 3$ in c_n are independent, we can get the expected value of c_n just by multiplying the expected value of its powers of 2,3. In particular:

$$\mathbb{E}(c_n) = \left(\frac{1}{16} + \frac{2 \cdot 7}{16} + \frac{4}{2}\right)\left(\frac{1}{3} + \frac{2 \cdot 3}{3}\right) = \frac{329}{48}$$

There are $\phi(210) = 48$ nonzero values of c_n, so our answer is $48 \cdot \frac{329}{48} = \boxed{329}$. □

Example 3.8 (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 $n^{n+1} + 1$.

Solution. To start, we see that all odd m work. Set $n = m-1$ so that $n^{n+1} \equiv (-1)^m \equiv -1 \pmod{m}$, as desired.

Now, we will find which even m work. Clearly, n must be odd in this case. When $n = 2k + 1$,

$$n^{n+1} + 1 \equiv (2k+1)^{2k+2} + 1 = ((2k+1)^{k+1})^2 + 1 \equiv 2 \pmod{4}.$$

Now, since $n^{n+1} + 1$ is the sum of two perfect squares, all odd prime factors must be 1 mod 4. Therefore, all odd prime factors of m are 1 mod 4. Since m is even and $m \leq 50$, all prime factors are less than 25. The possible prime factors are $5, 13, 17$. Therefore, the only possible even m that could work are $m = 2, 10, 26, 34, 50$. We can find a construction in each of these cases. Note that if $n^2 \equiv -1 \pmod{\frac{m}{2}}$ and $n \equiv 1 \pmod{4}$, then $n+1 \equiv 2 \pmod{4}$, so

$$n^{n+1} \equiv (-1)^{\text{odd}} \equiv -1 \pmod{\frac{m}{2}}.$$

Also $n^{n+1} + 1 \equiv 1 \pmod{2}$, so we can conclude m divides $n^{n+1} + 1$ by the Chinese Remainder Theorem. The existence of such an n is because all odd prime factors of m are 1 mod 4 (We will discuss more about this in next week's handout!). From this, we can complete our constructions:

- For $m = 2$, let $n = 1$.
- For $m = 10$, let $n \equiv 1 \pmod{4}$ and $n \equiv 2 \pmod{5}$
- For $n = 26$, let $n \equiv 1 \pmod{4}$ and $n \equiv 5 \pmod{13}$
- For $n = 34$, let $n \equiv 1 \pmod{4}$ and $n \equiv 4 \pmod{17}$
- for $n = 50$, let $n \equiv 1 \pmod{4}$ and $n \equiv 7 \pmod{25}$

Therefore, our final answer is

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

□

Example 3.9 (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 $n - 1$.

Solution. Let $M = 2013m$. We want to find M such that $n^n \equiv 1 \pmod{M}$ implies $n \equiv 1 \pmod{M}$. It is clear that $\gcd(n, M) = 1$. We begin by proving the following key lemma:

Lemma 3.10
For any prime p, we have $p \mid M$ if and only if every prime factor of $p - 1$ divides M.

Proof. We will first show that this condition is necessary. Suppose otherwise, that we have primes p, q such that $p|M$, $q|p-1$, $q \nmid M$. Let k be the largest positive integer such that $p^k|M$. Consider an arbitrary primitive root $g \bmod p^k$. Let $a \equiv g^{p^{k-1}\frac{p-1}{q}} \pmod{p^k}$ so that $a^q \equiv 1 \pmod{p^k}$ and $a \not\equiv 1 \pmod{p}$. Now, we let n be a value such that $n \equiv 1 \pmod{\frac{M}{p^k}}$, $n \equiv a \pmod{p^k}$, and $n \equiv 0 \pmod{q}$. Because these modulos are relatively prime, such an n exists by the Chinese Remainder Theorem. Now, we note that n satisfies $M|n^n - 1$ and $M \nmid n - 1$, a contradiction.

Now, we can easily show that this condition is sufficient. Suppose that $n^n \equiv 1 \pmod{M}$. We will show $n \equiv 1 \pmod{M}$. It suffices to show this for every prime power dividing M. Consider a prime p dividing M, and let p^k be the largest power dividing M. Since, $n^n \equiv 1 \pmod{M}$, we have $\gcd(n, M) = 0$, which implies $\gcd(n, p^{k-1}(p-1)) = 1$ because every prime factor of $p - 1$ divides M. Since $n^n \equiv 1 \pmod{p^k}$, we see $\mathrm{ord}_{p^k} n \mid n$. However, we also have $\mathrm{ord}_{p^k}(n) \mid \phi(p^k) = p^{k-1}(p-1)$. Therefore, because n and $p^{k-1}(p-1)$ are relatively prime, we can conclude that $\mathrm{ord}_{p^k}(n) = 1$, as desired. Thus, our lemma is proven. □

Now, since 3 divides $M = 2013m$, we must have $2 \mid M$. Also, since 11 divides $2013m$, we must have $5 \mid m$. Therefore, $10 \mid m$. Let $m = 10k$ so that

$$M = 20130k = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 61 \cdot k.$$

From the given range, k can go from 1 to 30. We can check the condition in the lemma for all of the prime from 1 to 30 first (If p_1, p_2, ..., p_i, satisfy the condition separately, then $p_1 \cdot p_2 \cdots p_i$ clearly satisfies it too). We see that the only prime number that does not satisfy the condition is 29. Therefore, every value of k from 1 to 30 works, except 29. Our final answer is

$$10(1 + 2 + 3 + \cdots + 28 + 30) = \boxed{4360}.$$

□

Example 3.11 (China 2009)
Find all pairs of primes p, q such that $pq \mid 5^p + 5^q$.

Solution. First's, let's consider the case $p = q$. Then, we have $p^2 \mid 2 \cdot 5^p$. Since $2 \cdot 5^p$ only has the prime divisors $2, 5$ and is not a multiple of 4, we must have $p = q = 5$.

We now consider $p \neq q$. Let's consider if either of p, q is 5. WLOG, let $q = 5$. Then, we have $5p \mid 5^p + 5^5$. We need $5^p + 5^5 \equiv 0 \pmod{p}$, but by FLT, $5^p + 5^5 \equiv 5 + 5^5 \pmod{p}$.

This implies $p \mid 5 + 5^5 = 3130 = 2 \cdot 5 \cdot 313$, so $p = 2, 313$. Accounting for permutations, the pairs in this case are $(2, 5), (313, 5), (5, 2), (5, 313)$.

Now, we have the case of neither p, q is equal to 5. By FLT, we have $5^p + 5^q \equiv 5 + 5^q \equiv 5(1 + 5^{q-1}) \equiv 0 \pmod{p}$. Therefore, $p \mid 1 + 5^{q-1}$, so

$$5^{q-1} \equiv -1 \pmod{p} \implies 5^{2q-2} \equiv 1 \pmod{p}.$$

If $p \neq 2$, we have $\text{ord}_p(5) \mid 2(q-1)$ and $\text{ord}_p(5) \nmid q-1$ (In the case $p = 2$, we see $5^{q-1} \equiv 1 \pmod{p}$ as well). Define $\nu_2(n)$ to be the largest positive integer k such that $2^k \mid n$. We must have $\nu_2(\text{ord}_p(5)) = 1 + \nu_2(q-1)$. However, from FLT, we know $\text{ord}_p(5) \mid \phi(p) = p-1$. Therefore,

$$1 + \nu_2(q-1) = \nu_2(\text{ord}_p(5)) \leq \nu_2(p-1).$$

We similarly have

$$5^{p-1} \equiv -1 \pmod{q} \implies 5^{2p-2} \equiv 1 \pmod{q}.$$

From this, assuming $q \neq 2$, we can similarly obtain $1 + \nu_2(p-1) \leq \nu_2(q-1)$. Adding this inequality with the inequality above is a direct contradiction. Therefore, one of p, q must be equal to 2. WLOG, let $q = 2$. Then, we have $2p \mid 5^p + 5^2$, and clearly $2 \mid 5^p + 5^2$, so we just need $p \mid 5^p + 5^2$. We have $5^p + 5^2 \equiv 5 + 5^2 \pmod{p}$, so $p \mid 30$. Thus, we need $p = 3$, as we have already accounted for the cases $p = 5$ and $p = q$. Accounting for permutations, we have the solutions $(2, 3), (3, 2)$.

To conclude, all of the solutions are $\boxed{(5,5), (2,5), (5,2), (5,313), (313,5), (2,3), (3,2)}$.

□

§4 Problems

Problem 4.1 (2020 HMMT Combinatorics #2)**.** How many positive integers at most 420 leave different remainders when divided by each of 5, 6, and 7?

Problem 4.2 (2017 AMC 12 #21)**.** 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?

Problem 4.3 (Fermat Christmas Theorem)**.** Let $p \equiv 3 \pmod 4$ be a prime, and let a and b be positive integers such that p divides $a^2 + b^2$. Show that $p \mid a$ and $p \mid b$.

Problem 4.4 (Wilson)**.** Prove that $(p-1)! \equiv -1 \pmod p$.

Problem 4.5. Prove that if $p \equiv 1 \pmod 4$, then there is an element $x \in \mathbb{Z}/p\mathbb{Z}$ such that $x^2 \equiv -1 \pmod p$.

Problem 4.6 (2013 AIME I #11)**.** Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

(a) If 16, 15, or 14 students are present, then in each case all the blocks can be distributed in equal numbers to each student, and

(b) There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.

Problem 4.7 (2018 AIME I #11)**.** Find the least positive integer n such that when 3^n is written in base 143, its two right-most digits in base 143 are 01.

Problem 4.8 (2001 AIME I #10)**.** How many positive integer multiples of 1001 can be expressed in the form $10^j - 10^i$, where i and j are integers and $0 \leq i < j \leq 99$?

Problem 4.9 (2011 AIME I #11)**.** Let R be the set of all possible remainders when a number of the form 2^n, n a nonnegative integer, is divided by 1000. Let S be the sum of all elements in R. Find the remainder when S is divided by 1000.

Problem 4.10. Find all integers $n \geq 1$ such that n divides $2^n - 1$.

Problem 4.11. Let p be a prime and n a positive integer. Determine the remainder when $1^n + 2^n + \cdots + (p-1)^n$ is divided by p, as a function of n,and p.

Problem 4.12. Find all integers $n \geq 1$ such that n divides $2^{n-1} + 1$.

Problem 4.13 (Balkan)**.** Let n be a positive integer with $n \geq 3$. Show that $n^{n^{n^n}} - n^{n^n}$ is divisible by 1989.

Problem 4.14 (Euler)**.** Prove that all factors of $2^{2^n} + 1$ are of the form $k \cdot 2^{n+1} + 1$.

Problem 4.15 (2000 IMO Shorlist N1)**.** Determine all positive integers $n \geq 2$ that satisfy the following condition: for a and b relatively prime to n we have $a \equiv b \pmod n$ if and only if $ab \equiv 1 \pmod n$.

Problem 4.16 (2006 China TST)**.** Find all positive integers a and n for which n divides $(a+1)^n - a^n$.

Problem 4.17 (2005 IMO Shorlist N6)**.** Let a, b be positive integers such that $b^n + n$ is a multiple of $a^n + n$ for all positive integers n. Prove that $a = b$.

Problem 4.18 (USA TST 2003/3)**.** Find all ordered prime triples (p, q, r) such that $p \mid q^r + 1$, $q \mid r^p + 1$, and $r \mid p^q + 1$.