Lesson 13: Advanced Number Theory

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

September 2020

Quadratic Residues

- When working with naturals, it is easy to tell if a number is a square. However, the same is not true when working modulo n
- For example, 3 certainly doesn't look like a square, but when working (mod 11), we actually have $5^2 \equiv 3 \pmod{11}$
- Knowing whether or not we can take the square root of a number turns out to be a really useful property, so we give such residues a special name:

Definition of QRs

Let p be a prime number. We say $a \pmod{p}$ is a *quadratic residue* if there exists some integer x such that $x^2 \equiv a \pmod{p}$.

Quadratic Residues

Number of QRs

For an odd prime p, there are exactly $\frac{p+1}{2}$ quadratic residues.

- Let's begin by squaring every residue mod p. When do things intersect?
- If $x^2 \equiv y^2 \pmod{p}$, we have $(x-y)(x+y) \equiv 0 \pmod{p}$. Hence, the squares of two distinct residues are equal if and only if they are negatives of each other
- So, if we square all p residues, we get the QR 0 and $p-1$ nonzero QRs which pair up to form $\frac{p-1}{2}$ distinct residues
- Hence, we have $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ QRs

Quadratic Residues

- To facilitate our discussion on QRs, we introduce the notion of the *Legendre Symbol*:

Legendre Symbol

Let S be the set of quadratic residues modulo a prime p. Then, for an integer a we define the *Legendre symbol* to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \not\equiv 0 \pmod{p} \text{ and } a \in S \\ -1 & a \notin S \\ 0 & a \equiv 0 \pmod{p} \end{cases}.$$

- Surprisingly, there exists a closed form for the Legendre Symbol

Legendre Symbol

Euler's Criterion

We have $\left(\frac{x}{p}\right) \equiv x^{\frac{p-1}{2}} \pmod{p}$

- The result is obvious for $x = 0$. For nonzero x, remember we learned last week that we can always write $x = \zeta^k$ where ζ is a primitive root
- Now, we have that $x^{\frac{p-1}{2}} = \zeta^{\frac{k(p-1)}{2}}$. The exponent is $\frac{p-1}{2} \pmod{p-1}$ if k is odd and 0 otherwise. So,

$$RHS = \begin{cases} -1 & \text{if } 2 \nmid k \\ 1 & \text{if } 2 | k \end{cases}$$

- If k is even, then x is obviously a QR since it is the square of $\zeta^{k/2}$
- If k is odd, suppose the contrary, namely that $x = y^2$. Let $y = \zeta^j$. What does this give?

Legendre Symbol

- We now have $\zeta^k \equiv \zeta^{2j} \implies \zeta^{k-2j} \equiv 1 \pmod{p}$. Why is this a problem?
- ζ is a primitive root, so we should have $p-1 | k-2j$, but $p-1$ is even and $k-2j$ is odd. So, y does not exist and x is an NQR
- So, both sides are 1 if k is even and both sides are -1 if k is odd, as desired.
- Using this, we can prove a very nonintuitive corollary

Legendre Symbol

Multiplicativity

The Legendre symbol is multplicative. That is, we have

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

- Just plug into Euler's Criterion!
- $a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}}$, as desired. $\square$
- Finally, we will prove the most celebrated result regarding quadratic residues, dubbed Quadratic Reciprocity. Buckle your seatbelts!

Quadratic Residues

Quadratic Reciprocity

For distinct odd primes p, q,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

- Before attempting to prove this beautiful result, we begin with a lemma

Quadratic Reciprocity

Eisenstein's Lemma

Given odd primes p, q, we have that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_u \lfloor qu/p \rfloor}$$

where u ranges over all **even** nonzero residues

- Define r_u over all even u with $0 < u < p$ to be the remainder when qu is divided by p. Can you say anything about $(-1)^{r_u} \cdot r_u$?
- If r_u is even, it is r_u. Otherwise, its residue is $p - r_u$. Either way, the residue of $(-1)^{r_u} \cdot r_u$ is even
- Can we ever have $(-1)^{r_u} \cdot r_u \equiv (-1)^{r_v} \cdot r_v$ for different u, v?

Quadratic Reciprocity

- If this were true, then $r_u \equiv \pm r_v \pmod{p}$, so $q(u \pm v) \equiv 0 \pmod{p}$. Why can this not be true?
- u, v distinct so we need $u + v = p$. But, u, v are both even and p is odd, so this is impossible
- Hence, $(-1)^{r_u} \cdot r_u$ is always even, and all u produce distinct values. What does this tell us?
- The set $(-1)^{r_u} \cdot r_u$ is just a permutation of the even residues!
- So, we have that

$$\prod_u u \equiv \prod_u (-1)^{r_u} \cdot r_u \equiv (-1)^{\sum r_u} \cdot \prod_u qu \pmod{p}$$

- Cancelling out like terms,

$$1 \equiv q^{\frac{p-1}{2}} (-1)^{\sum r_u} \equiv \left(\frac{q}{p}\right) (-1)^{\sum r_u} \implies \left(\frac{q}{p}\right) = (-1)^{\sum r_u}$$

Quadratic Reciprocity

- We are almost done. How can we relate r_u and $\left\lfloor \frac{qu}{p} \right\rfloor$?
- Note that

$$\left\lfloor \frac{qu}{p} \right\rfloor = \frac{qu - r_u}{p} \implies r_u = p \left\lfloor \frac{qu}{p} \right\rfloor - qu$$

- qu is even and p is odd, so $r_u \equiv \left\lfloor \frac{qu}{p} \right\rfloor \pmod 2$
- Hence, $\left(\frac{q}{p}\right) = (-1)^{\sum r_u} = (-1)^{\sum \lfloor qu/p \rfloor}$, as desired. $\square$
- Unfortunately, the lemma is still pretty unwieldy as of now. In particular, the fact that u has to be even is pretty annoying. Let's see if we can make it simpler.

Quadratic Reciprocity

- Claim:

$$\sum_{\substack{u<p \\ 2|u}} \left\lfloor \frac{qu}{p} \right\rfloor \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{qi}{p} \right\rfloor \pmod 2$$

- Note that $\left\lfloor \frac{qu}{p} \right\rfloor + \left\lfloor \frac{q(p-u)}{p} \right\rfloor = \frac{qu-r(qu)}{p} + \frac{q(p-u)-r(q(p-u))}{p}$. What is $r(qu) + r(q(p-u))$?
- $qu, q(p-u)$ are negatives mod p, so their remainders add to p. Hence,

$$\left\lfloor \frac{qu}{p} \right\rfloor + \left\lfloor \frac{q(p-u)}{p} \right\rfloor = \frac{qu + q(p-u) - p}{p} = q - 1$$

- $q-1$ is even! This means $\left\lfloor \frac{qu}{p} \right\rfloor$ and $\left\lfloor \frac{q(p-u)}{p} \right\rfloor$ have the same parity! Using this, how can we prove the claim?

Quadratic Reciprocity

- $$\sum_{\substack{u<p \\ 2|u}} \left\lfloor \frac{qu}{p} \right\rfloor \equiv \sum_{\substack{u<p/2 \\ 2|u}} \left\lfloor \frac{qu}{p} \right\rfloor + \sum_{\substack{u>p/2 \\ 2|u}} \left\lfloor \frac{q(p-u)}{p} \right\rfloor \pmod 2$$

  What is the second sum?

- u ranges over evens $> p/2$, so $p-u$ ranges over odds $< p/2$. So, we are adding $\left\lfloor \frac{qu}{p} \right\rfloor$ over odd numbers less than $p/2$!
- So, the sum we wrote is none other than

$$\sum_{\substack{u<p/2 \\ 2|u \text{ or } 2\nmid u}} \left\lfloor \frac{qu}{p} \right\rfloor = \sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{qu}{p} \right\rfloor$$

and the claim is proven

Quadratic Reciprocity

- Using this claim, we greatly simplify our expression. In particular, we now have

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{qu}{p} \right\rfloor}$$

- So, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\sum \left\lfloor \frac{qu}{p} \right\rfloor + \sum \left\lfloor \frac{pu}{q} \right\rfloor}$. It would be convenient if

$$\sum_{u=1}^{\frac{p-1}{2}} \left\lfloor \frac{qu}{p} \right\rfloor + \sum_{u=1}^{\frac{q-1}{2}} \left\lfloor \frac{pu}{q} \right\rfloor = \frac{(p-1)(q-1)}{4}$$

  In fact it is! Can you see why without writing anything down?

- Consider the rectangle in the coordinate plane bounded by $x = 0, p/2$ $y = 0, q/2$. What does the first sum count?

Quadratic Reciprocity

- $\left\lfloor \frac{qu}{p} \right\rfloor$ counts the number of lattice points with x coordinate u which are under line $y = \frac{q}{p}x$. So, the first sum counts the number of lattice points in the rectangle under $y = \frac{p}{q}x$
- $\left\lfloor \frac{pu}{q} \right\rfloor$ counts the number of lattice points with y coordinate u which are to the left of $x = \frac{p}{q}y$. This is the same region as the lattice points above $y = \frac{q}{p}x$.
- No lattice points lie on $y = \frac{q}{p}x$, so the two sums together count the number of lattice points in the rectangle, which is just $\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$, as desired.
- Now, substituting this equality back into our initial expression, we get that $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$, as desired.

Problem of the Week

PotW

Let $f(x) = x^2 + 5x + 3$. Denote P as the remainder when $\prod_{n=1}^{2016} f(n)$ is divided by 2017 and let Q be the number of distinct residues $f(n)$ achieves mod 2017. Find the last 3 digits of PQ.

- We begin by finding Q. How can we rewrite f to make this task easier?
- $f(x) = \left(x + \frac{5}{2}\right)^2 - \frac{13}{4}$
- $x + \frac{5}{2}$ ranges over all residues, so $\left(x + \frac{5}{2}\right)^2$ ranges over all QRs
- We already know that there are $\frac{2017+1}{2} = 1009$ QRs, so $Q = 1009$
- Now, we need to compute P. We can actually use the same form we used to calculate Q. First, consider

$$R = \prod_{n=0}^{2016} \left(n + \frac{5}{2}\right)^2 - \frac{13}{4}$$

PotW

- Reindexing, $R = \prod_{n=0}^{2016} \left(n^2 - \frac{13}{4}\right)$. How many times does each QR appear in this product?
- Each QR appears twice, besides 0. So, we can rewrite the product as

$$-\frac{13}{4}\left(\prod_{\left(\frac{n}{2017}\right)=1} n - \frac{13}{4}\right)^2 = -\frac{13}{4}\left(\prod_{\left(\frac{n}{2017}\right)=1} \frac{13}{4} - n\right)^2$$

- It would be nice if we had a polynomial with roots the quadratic residues. That way, we would have $R = -\frac{13}{4}P\left(\frac{13}{4}\right)^2$. Do we know P?
- Remember that $x^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ if and only if x is a nonzero QR. Aha! This is the P we are looking for. So,

$$R = -\frac{13}{4}\left(\left(\frac{13/4}{2017}\right) - 1\right)^2$$

PotW

- $\left(\frac{13/4}{2017}\right) = \left(\frac{13}{2017}\right)$. How can we find this?
- Using quadratic reciprocity,

$$\left(\frac{13}{2017}\right)\left(\frac{2017}{13}\right) = 1 \implies \left(\frac{13}{2017}\right) = \left(\frac{2}{13}\right) = -1$$

- Hence,

$$R = -\frac{13}{4} \cdot (-1-1)^2 = -13$$

- We have that $R = f(0)P = 3P \implies P \equiv -\frac{13}{3} \equiv 668 \pmod{2017}$
- So, our answer is

$$668 \cdot 1009 \equiv \boxed{012} \pmod{1000}$$

Quadratic Residues

Folklore

Find the number of ordered pairs (x, y) with $0 \leq x, y < 2027$ which satisfy

$$x^2 + y^2 \equiv 1 \pmod{2027}$$

- For a fixed y, how many solutions for x are there?
- If $1 - y^2 = 0$, there is 1. If $1 - y^2$ is a nonzero QR, there are 2, and if $1 - y^2$ is an NQR, there are 0. What does this remind you of?
- These numbers correspond to $\left(\frac{1-y^2}{p}\right) + 1$ (define $p = 2027$)
- So, the number of solutions is just

$$\sum_{y=0}^{2026} \left(\left(\frac{1-y^2}{p} \right) + 1 \right) = 2028 + \sum_{y=1}^{2026} \left(\frac{1-y^2}{p} \right)$$

How can we deal with the sum on the RHS? (call it S.)

Quadratic Residues

- One thing we can do is substitute $y \to \frac{1}{y}$. This is a bijection on the nonzero residues, so reindexing gives us

$$S = \sum_{y=1}^{2026} \left(\frac{1-(1/y)^2}{p} \right) = \sum_{y=1}^{2026} \left(\frac{1/y^2}{p} \right) \left(\frac{y^2-1}{p} \right)$$

  How can we simplify this sum?

- Remember that $1/y^2$ is a nonzero square, so this is just $\sum_{y=1}^{2026} \left(\frac{y^2-1}{p} \right)$
- All the arguments are negative that of our initial expression -

$$S = \sum_{y=1}^{2026} \left(\frac{y^2-1}{p} \right) = \left(\frac{-1}{p} \right) \sum_{y=1}^{2026} \left(\frac{1-y^2}{p} \right) = \left(\frac{-1}{p} \right) S$$

Quadratic Residues

- Do we know $\left(\frac{-1}{p}\right)$?
- p is 3 (mod 4), so it is -1. Hence, $S = -S \implies S = 0$
- So, the number of solutions is $2028 + S = \boxed{2028}$.

When 2 is a quadratic residue

Theorem

For an odd prime p,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{1}{8}(p^2-1)}$$

- This means 2 is a quadratic residue when $p \equiv 1, 7 \pmod 8$, and is a quadratic nonresidue when $p \equiv 3, 5 \pmod 8$.

Quadratic Residues

Adithya

The positive integers a and b are such that the numbers $15a + 16b$ and $16a - 15b$ are both squares of positive integers. Let S be the smallest possible value of $a + b$. Compute $S \pmod{1000}$.

- Let $15a + 16b = x^2$ and $16a - 15b = y^2$.
- What are a and b in terms of x and y?
- Solve to get $a = \frac{15x^2+16y^2}{481}$ and $b = \frac{16x^2-15y^2}{481}$.
- What modular congruences can you write from these equations?
- For example, $15x^2 + 16y^2 \equiv 0 \pmod{13} \implies 2x^2 \equiv -3y^2 \pmod{13}$.
- Multiply both sides by 7 to get $x^2 \equiv 5y^2 \pmod{13}$.
- If $13 \nmid y$, we can divide so that $\left(\frac{x}{y}\right)^2 \equiv 5 \pmod{13}$. 5 is a quadratic residue mod 13. Does this agree with the result from quadratic reciprocity?

Quadratic Residues

- From quadratic reciprocity, $\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{\frac{1}{4}\cdot 12\cdot 4} = 1$.
- We know $\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$.
- So, $13 \mid y$, and this implies $13 \mid x$.
- Now, we also have $15x^2 + 16y^2 \equiv 0 \pmod{37} \implies 15x^2 \equiv -16y^2 \pmod{37}$.
- Multiply by $15^{-1} \equiv 5$ to get $x^2 \equiv -6y^2 \pmod{37}$. If $37 \nmid y$, then -6 is a quadratic residue mod 37.
- $\left(\frac{-6}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)\left(\frac{3}{37}\right)$
- Since $37 \equiv 5 \pmod{8}$, -1 is a QR but 2 is not.
- Is 3 a quadratic residue?
- $\left(\frac{3}{37}\right)\left(\frac{37}{3}\right) = 1 \implies \left(\frac{3}{37}\right) = 1$
- Thus, 3 is a QR, so we get $\left(\frac{-6}{37}\right) = -1$. So, $37 \mid y$ and $37 \mid x$.
- As $481 \mid x, y$, $a + b$ is minimized when $x = y = 481$. The smallest possible value of $a + b$ is $32 \cdot 481 \equiv \boxed{392} \pmod{1000}$.

Jacobi Symbol

- While the Legendre symbol is multiplicative of the top, we can extend this notion to the *Jacobi symbol* so that it is multiplicative on both the top and the bottom.
- In order words, the Jacobi symbol would also satisfy

$$\left(\frac{a}{mn}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right).$$

- A few important facts about the Jacobi symbol are the following:
  1. $\left(\frac{a}{n}\right) = 0$ when $\gcd(a, n) \neq 1$
  2. $\left(\frac{a}{n}\right) = \left(\frac{b}{m}\right)$ when $a \equiv b \pmod{n}$.
- An alternate, but equivalent, definition of the Jacobi symbol $\left(\frac{a}{n}\right)$ is the product of the Legendre symbols corresponding to the (not necessarily distinct) prime factors of $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1}\left(\frac{a}{p_2}\right)^{e_2}\cdots\left(\frac{a}{p_k}\right)^{e_k}$$

Jacobi Symbol

Theorem (Quadratic reciprocity with Jacobi symbols)

If m and n are odd positive integers with $\gcd(m, n) = 1$, *then*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}.$$

Also, we have

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{1}{2}(m-1)}, \qquad \left(\frac{2}{m}\right) = (-1)^{\frac{1}{8}(m^2-1)}.$$

Warning!

It is important to note that the Jacobi symbol does not necessarily detect quadratic residues. That is, if $\left(\frac{a}{m}\right) = -1$ and $\left(\frac{a}{n}\right) = -1$, then $\left(\frac{a}{mn}\right) = 1$, but this does not mean a is a quadratic residue mod mn.

Quadratic reciprocity with Jacobi symbols

2019 PRIMES M5

Exhibit a function $s : \mathbb{Z}_{>0} \to \mathbb{Z}$ with the following property: if a and b are positive integers such that $p = a^2 + b^2$ is an odd prime, then

$$s(a) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

The right-hand side is known as the *Jacobi symbol* $\left(\frac{a}{p}\right)$.

- We want a function that is always equal to the Jacobi symbol $\left(\frac{a}{p}\right)$.
- We want to apply quadratic reciprocity. How can we do that?
- Remove powers of 2 from a!
- Remember that if $a = 2^k a_1$, where a_1 is odd, then

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{a_1}{p}\right)$$

2019 PRIMES M5

- Let's do casework on the value of k, starting with $k = 0$ (a is odd).
- Since $p = a^2 + b^2$, we must have $p \equiv 1 \pmod 4$ since $0, 1$ are the only quadratic residues mod 4.
- Now, by quadratic reciprocity, $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{\frac{1}{4}(a-1)(p-1)} = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$
- We can set $s(a) = 1$ when a is odd.
- Now, let's do the case when $a = 1$ or $a = 2a_1$, where a_1 is odd.
- What is $p \pmod 8$?
- $a \equiv 2 \pmod 4$, so $a^2 \equiv 4 \pmod 8$. b must be odd, so $b^2 \equiv 1 \pmod 8$. Therefore, $p \equiv 5 \pmod 8$.
- 2 is not a quadratic residue mod p.
- $\left(\frac{a_1}{p}\right)\left(\frac{p}{a_1}\right) = (-1)^{\frac{1}{4}(a_1-1)(p_1-1)} = 1$
- $\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a_1}{p}\right) = -1 \cdot \left(\frac{p}{a_1}\right) = -1 \cdot \left(\frac{4a_1^2+b^2}{a_1}\right) = -1 \cdot \left(\frac{b^2}{a_1}\right) = -1$

- So for $a \equiv 2 \pmod 4$, we can always set $s(a) = -1$.
- Let's move on to when there are at least 2 powers of 2 in a.
- Note that from the work above, for all values of $k \geq 2$, $a^2 \equiv 0 \pmod 8$ and $b^2 \equiv 1 \pmod 8$, so $p \equiv 1 \pmod 8$.
- 2 is a quadratic residue.
- By quadratic reciprocity, $\left(\frac{a_1}{p}\right)\left(\frac{p}{a_1}\right) = (-1)^{\frac{1}{4}(a_1-1)(p_1-1)} = 1$
- $\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{a_1}{p}\right) = \left(\frac{a_1}{p}\right) = \left(\frac{p}{a_1}\right) = \left(\frac{2^{2k}a_1^2+b^2}{a_1}\right) = \left(\frac{b^2}{a_1}\right) = 1$
- When $4 \mid a$, we can let $s(a) = 1$.
- To conclude,

$$s(a) = \begin{cases} 1 & a \equiv 1 \pmod 2 \\ -1 & a \equiv 2 \pmod 4 \\ 1 & a \equiv 0 \pmod 4 \end{cases}$$

p-adic Valuations

- Let p be a prime and n be a positive integer
- The *p-adic valuation* of n is the largest integer k such that n is divisible by p^k
- We denote this number by $\nu_p(n)$
- For example, $\nu_2(96) = 5$ as 2^5 is the largest power of 2 dividing 96
- A basic property is that $\nu_p(ab) = \nu_p(a) + \nu_p(b)$
- We also have $\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b))$
- If $\nu_p(a) \neq \nu_p(b)$ then equality holds: $\nu_p(a+b) = \min(\nu_p(a), \nu_p(b))$
- One useful theorem you may have seen is *Legendre's Formula*, which states that

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots .$$

p-adic Valuations

- This can be seen as follows: write $n! = 1 \cdot 2 \cdots n$
- Each multiple of p in this product increases the ν_p count by 1; there are $\left\lfloor \frac{n}{p} \right\rfloor$ such multiples
- Each multiple of p^2 in the product contributes *again* to the ν_p count: there are $\left\lfloor \frac{n}{p^2} \right\rfloor$ such multiples
- And so on, for the final sum of $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots$
- Another version of Legendre says that $\nu_p(n!) = \frac{n - s_p(n)}{p-1}$, where $s_p(n)$ is the sum of the digits of n in base p
- This can be proven by writing $n = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0$ in base p, and then showing

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots = \frac{n - s_p(n)}{p-1}$$

p-adic Valuations

Lifting the Exponent lemma

Let p, a, b, and n be positive integers satisfying all three properties below:

- p is an *odd* prime,
- p does not divide a or b, and
- p divides $a - b$.

Then

$$\nu_p(a^n - b^n) = \nu_p(a - b) + \nu_p(n).$$

- We will induct on $\nu_p(n)$
- Base case $\nu_p(n) = 0$, i.e. $p \nmid n$
- Then we need $\nu_p(a^n - b^n) = \nu_p(a - b)$
- Equivalently p does not divide $\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2}b + \cdots + b^{n-1}$
- Since $p|a - b$ we have $a \equiv b \pmod{p}$

Lifting the Exponent lemma

- We have

$$a^{n-1}+a^{n-2}b+\cdots+b^{n-1} \equiv a^{n-1}+a^{n-2}\cdot a+\cdots+a^{n-1} \equiv na^{n-1} \pmod{p}$$

- a and n are both not divisible by p by assumption, so this isn't divisible by p either
- The base case is done; let's move on to the inductive step
- Suppose the lemma holds when $\nu_p(n) = k$; it suffices to show it holds when $\nu_p(n) = k+1$
- If $\nu_p(n) = k+1$ let $N = \frac{n}{p}$ so $\nu_p(N) = k$
- By the inductive hypothesis we have $\nu_p(a^N - b^N) = \nu_p(a-b) + \nu_p(N)$
- We want $\nu_p(a^{pN} - b^{pN}) = \nu_p(a-b) + \nu_p(pN)$
- Subtract: it suffices to show $\nu_p(a^{pN} - b^{pN}) - \nu_p(a^N - b^N) = \nu_p(pN) - \nu_p(N)$

Lifting the Exponent lemma

- The RHS is 1, so we want $\nu_p(a^{pN} - b^{pN}) - \nu_p(a^N - b^N) = 1$
- Equivalently, $\frac{a^{pN}-b^{pN}}{a^N-b^N}$ is divisible by p but not p^2
- Since $p|a-b$, we have $p|a^N - b^N$
- Let $b^N = m$, $a^N = m + pk$; then $p \nmid m$
- Then $\frac{a^{pN}-b^{pN}}{a^N-b^N} = \frac{1}{pk}\left((M+pk)^p - M^p\right)$
- Binomial Theorem:
  $\frac{1}{pk}\left(\binom{p}{1}M^{p-1}pk + \binom{p}{2}M^{p-2}(pk)^2 + \binom{p}{3}M^{p-3}(pk)^3 + \cdots + (pk)^p\right)$
- $= \binom{p}{1}M^{p-1} + \binom{p}{2}M^{p-2}pk + \binom{p}{3}M^{p-3}(pk)^2 + \cdots + (pk)^{p-1}$
- Clearly divisible by p: each term is divisible by p
- All terms starting from the third term are divisible by p^2: they have a factor of p^2
- Second term also divisible by p^2: $\binom{p}{2}$ is divisible by p (since p is odd!)
- First term not divisible by $p^2 \implies$ sum not divisible by p^2

p-adic Valuations

2020 AIME I #12

Let n be the least positive integer for which $149^n - 2^n$ is divisible by $3^3 \cdot 5^5 \cdot 7^7$. Find the number of positive divisors of n.

- Want difference of n^{th} powers to be divisible by large prime powers $\implies$ LTE
- Let's use LTE for the prime 3: 3 is odd, $3 \nmid 149, 2$, and $3 \mid 149 - 2$
- $\nu_3(149^n - 2^n) = \nu_3(149 - 2) + \nu_3(n) = \nu_3(n) + 1$
- $3^3 | 149^n - 2^n \implies \nu_3(n) \geq 2 \implies 3^2 | n$
- Now use LTE on 7: 7 is odd, $7 \nmid 149, 2$, and $7 | 149 - 2$
- $\nu_7(149^n - 2^n) = \nu_7(149 - 2) + \nu_7(n) = \nu_7(n) + 2$
- $7^7 | 149^n - 2^n \implies \nu_7(n) \geq 5 \implies 7^5 | n$
- Now let's use LTE on 5

2020 AIME I #12

- We can't use LTE on 5: we don't have $5|149-2$
- In fact, we don't always have $5|149^n-2^n$; when does this happen?
- $149^n-2^n \equiv 4^n-2^n \equiv 2^n(2^n-1) \pmod 5$
- If $5|149^n-2^n$ then $5|2^n-1$ which occurs exactly when $4|n$
- Need $4|n$; let $n=4k$
- Now we can use LTE by writing $149^n-2^n=(149^4)^k-(2^4)^k$
- $\nu_5(149^{4k}-2^{4k})=\nu_5((149^4)^k-(2^4)^k))=\nu_5(149^4-2^4)+\nu_5(k)$
- Check that $\nu_5(149^4-2^4)=1$
- So $\nu_5(149^n-2^n)=\nu_5(k)+1=\nu_5(n)+1$
- If $5^5|149^n-2^n$ then $\nu_5(n)\geq 4 \implies 5^4|n$
- Combining, n must be a multiple of 3^2, 7^5, 4, and 5^4
- So n is a multiple of $2^2\cdot 3^2\cdot 5^4\cdot 7^5$
- n has at least $(2+1)(2+1)(4+1)(5+1)=\boxed{270}$ divisors

p-adic Valuations

IMO 2019/4

Find all pairs (k, n) of positive integers such that

$$k! = (2^n - 1)(2^n - 2)(2^n - 4)\dots(2^n - 2^{n-1})$$

- Factor RHS: pull out as many factors of 2 as possible
- $(2^n - 1)2(2^{n-1} - 1)2^2(2^{n-2} - 1)\cdots 2^{n-1}(2^1 - 1)$
- $2^{\frac{n(n-1)}{2}}(2^n - 1)(2^{n-1} - 1)\dots(2^1 - 1)$
- The 2-adic valuation of this is clearly $\frac{n(n-1)}{2}$
- So $\nu_2(k!) = \frac{n(n-1)}{2}$
- By Legendre $\nu_2(k!) = k - s_2(k) \leq k$
- So $k \geq \nu_2(k!) = \frac{n(n-1)}{2}$
- Actually, this means k needs to be quite large; maybe even too large

IMO 2019/4

- We have $k! \geq \left(\frac{n(n-1)}{2}\right)!$
- $k! = (2^n - 1)(2^n - 2)(2^n - 4)\ldots(2^n - 2^{n-1}) \leq 2^n \cdot 2^n \cdots 2^n = 2^{n^2}$
- So we have $2^{n^2} \geq \left(\frac{n(n-1)}{2}\right)!$
- This should not be true for large n: the LHS is multiplying n^2 copies of 2, while the RHS is a product of about $\frac{1}{2}n^2$ numbers, most of them much larger than 2
- We claim this actually implies $n < 6$; if $n \geq 6$ then $\left(\frac{n(n-1)}{2}\right)! > 2^{n^2}$
- Prove by induction: for $n = 6$ we have $15! > 2^{36}$
- (say, $15! > 7! \cdot 8^8 > 2^{12} \cdot 2^{24} = 2^{36}$)
- For the inductive step, suppose $\left(\frac{n(n-1)}{2}\right)! > 2^{n^2}$
- We want to show $\left(\frac{n(n+1)}{2}\right)! > 2^{(n+1)^2}$

IMO 2019/4

- We have $\left(\frac{n(n+1)}{2}\right)! > \left(\frac{n(n-1)}{2}\right)! \cdot \left(\frac{n(n-1)}{2}\right)^n > 2^{n^2}\left(\frac{n(n-1)}{2}\right)^n$
- Now to complete the induction we just need $2^{n^2}\left(\frac{n(n-1)}{2}\right)^n > 2^{(n+1)^2}$
- Equivalently $\left(\frac{n(n-1)}{2}\right)^n > 2^{2n+1}$
- Or $\frac{n(n-1)}{2} > 2^{2+\frac{1}{n}}$
- Since $n \geq 6$ we have $\frac{n(n-1)}{2} \geq 15$ and $2^{2+\frac{1}{n}} < 8$, done
- We've now proven that if $n \geq 6$ then $\left(\frac{n(n-1)}{2}\right)! > 2^{n^2}$
- We've also prove that if (k, n) satisfy the equation then $2^{n^2} \geq \left(\frac{n(n-1)}{2}\right)!$
- Thus if (k, n) is a solution to the equation then $n \leq 5$
- We can now manually solve the equation for these five values of n

IMO 2019/4

- $k! = (2^n - 1)(2^n - 2)(2^n - 4)\ldots(2^n - 2^{n-1})$
- $n = 1$: then $k! = 1$ so $k = 1$
- $n = 2$: then $k! = 6$ so $k = 3$
- $n = 3$: then $k! = 168$ which clearly has no solutions
- $n = 4$: then $k! = 20160$ which has no solutions ($7! = 5040$ and $8! = 40320$)
- $n = 5$: then $k! = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$ which has no solutions: since $31 | k!$ and 31 is prime we have $k \geq 31$, but this would force $29 | k!$ which is a contradiction
- So the only solutions are $\boxed{(1, 1) \text{ and } (3, 2)}$