Advanced Number Theory

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

9/9

§1 Quadratic Residues

When we are working with natural numbers, it is easy to tell if a number has a square root - just check if it is a perfect square. However, it is much harder when we are working with modular arithmetic. For example, 3 is definitely not a perfect square, yet in $\pmod 1$1, we have that $5^2 \equiv 3 \pmod{11}$, showing that it is a square under some modulos. As it is often important to determine whether a number actually has a square root, this motivates us to give perfect squares under modular arithmetic a special name:

Definition 1.1 (Quadratic residue)**.** Let p be a prime number. We say $a \pmod p$ is a *quadratic residue* if there exists some integer x such that $x^2 \equiv a \pmod p$.

Lemma 1.2 (number of quadratic residues)
For an odd prime p, there are exactly $\frac{p+1}{2}$ quadratic residues.

Proof. We can try constructing a set of $\frac{p+1}{2}$ quadratic residues. Note that $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are all quadratic residues. To show that they are distinct, note that if $a^2 \equiv b^2 \pmod p$ for distinct a, b, then $(a+b)(a-b) \equiv 0 \pmod p$. As $a \not\equiv b$, we must have $a + b \equiv 0 \pmod p$. However, for the perfect squares that we have listed above $0 < a + b < p$, so we have constructed $\frac{p+1}{2}$ distinct quadratic residues. To show that there are no other quadratic residues, note that $(p-x)^2 \equiv x^2 \pmod p$. □

We notice that quadratic residues occur in exactly half of the nonzero residues modulo p. To discuss further about quadratic residues, we will first introduce some notation.

Definition 1.3 (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

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

To determine whether a number is a quadratic residue, one method we can use is exponentiation.

Theorem 1.4 (Euler's criterion)
For an odd prime p, $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$.

Proof. The result is obvious when $a \equiv 0 \pmod{p}$, so assume otherwise. Let g be a primitive root. If a is a quadratic residue, then $a = g^{2k}$ for some k. In that case, $a^{\frac{p-1}{2}} \equiv g^{k(p-1} \equiv 1 \pmod{p}$ from Fermat's Little Theorem, as desired. If a is not a quadratic residue, then $a \equiv g^{2k+1}$ for some k. In that case, $a^{\frac{p-1}{2}} = g^{\frac{2k+1}{2}(p-1)} \not\equiv 1 \pmod{p}$. However, since $(a^{\frac{p-1}{2}})^2 \equiv 1 \pmod{p}$ by Fermat's Little Theorem again, and $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, we must have $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

Theorem 1.5

The Legendre symbol is multplicative. That is, we have

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

Proof. This is clear from Theorem 1.4. Note that

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

Since the Legendre symbol only takes the values $\{-1, 0, 1\}$ and p is an odd prime, we can conclude that the function is multiplicative. □

Now, we will discuss one of the most important results in the theory of quadratic residues, *quadratic reciprocity*.

Theorem 1.6 (Quadratic Reciprocity)

For distinct odd primes p, q,

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

Proof. We will present a clever proof by Eisenstein, which involves the following lemma.

Lemma 1.7 (Gauss)

Let a be an integer such that $p \nmid a$, let r_n be the unique integer congruent to $an \pmod{p}$ such that $|r_n|$ is minimum. Then, if $R = \{1 \le n \le \frac{p-1}{2} \mid r_n < 0\}$, we have $\left(\frac{a}{p}\right) = (-1)^{|R|}$.

Proof. For $1 \le i \le \frac{p-1}{2}$, there is a unique n such that r_n is equal to i or $-i$. To show this, note that if $|r_x| = |r_y|$, then $(r_x \pm r_y) = 0 \implies n(x \pm y) \equiv 0 \pmod{p}$, which cannot occur for $1 \le x, y \le \frac{p-1}{2}$. Therefore, each $|r_n|$ is distinct, and there are $\frac{p-1}{2}$ values of n. Since $1 \le |r_n| \le \frac{p-1}{2}$, each value is obtained exactly once, as desired. Now, this means

that

$$\begin{aligned}\left(\frac{p-1}{2}\right)! &= \prod_{1\le i\le \frac{p-1}{2}} i = \prod_{1\le n\le \frac{p-1}{2}, n\in R} (-r_n)\cdot \prod_{1\le n\le \frac{p-1}{2}, n\notin R} r_n \\ &= (-1)^{|R|}\prod_{n=1}^{\frac{p-1}{2}} r_n \\ &\equiv (-1)^R \prod_{n=1}^{\frac{p-1}{2}} (an) \\ &= (-1)^{|R|} a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod p\end{aligned}$$

Therefore, we see $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^{|R|} \pmod p$, so $\left(\frac{a}{p}\right) = (-1)^{|R|}$.

■

We can use this to prove another result about the Legendre symbol.

Lemma 1.8

We have that $\left(\frac{a}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p}\right\rfloor}$.

Proof. By the previous lemma, we have

$$\sum_{n=1}^{\frac{p-1}{2}} \left(an - \left\lfloor \frac{an}{p}\right\rfloor\right) = \sum_{1\le n\le \frac{p-1}{2}, n\in R} (r_n + p)\cdot \prod_{1\le n\le \frac{p-1}{2}, n\notin R} r_n = p|R| + \sum_{n=1}^{\frac{p-1}{2}} r_n.$$

Since $|r_n|$ takes all values from 1 to $\frac{p-1}{2}$.

$$\sum_{n=1}^{\frac{p-1}{2}} r_n = \sum_{n=1}^{\frac{p-1}{2}} |r_n| = \sum_{n=1}^{\frac{p-1}{2}} an \pmod 2.$$

Therefore, $p|R| \equiv |R| \equiv \sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p}\right\rfloor \pmod 2$, so

$$\left(\frac{a}{p}\right) = (-1)^{|R|} = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{an}{p}\right\rfloor}.$$

■

To compute this sum, we will use the following lemma.

Lemma 1.9

If a, b are odd positive integers such that $\gcd(a, b) = 1$,

$$\sum_{n=1}^{\frac{b-1}{2}} \left\lfloor \frac{an}{b}\right\rfloor + \sum_{n=1}^{\frac{a-1}{2}} \left\lfloor \frac{bn}{a}\right\rfloor = \frac{(a-1)(b-1)}{4}.$$

Proof. Consider the rectangle bounded by the axes and the lines $x = \frac{b}{2}$ and $y = \frac{a}{2}$. The first sum counts the number of lattice points that are below the line $y = \frac{a}{b}x$. The second sum counts the number of points above this line. Since there are no lattice points on this line inside the rectangle, as $\gcd(a, b) = 1$, the total sum is equal to the number of lattice points inside the rectangle or $\frac{(a-1)(b-1)}{4}$. ■

Combining all the lemmas above,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{n=1}^{\frac{p-1}{2}} \left\lfloor \frac{qn}{p} \right\rfloor} \cdot (-1)^{\sum_{n=1}^{\frac{q-1}{2}} \left\lfloor \frac{pn}{q} \right\rfloor} = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

□

We would also like to know how to determine whether -1 and 2 are quadratic residues.

Theorem 1.10 (Quadratic reciprocity extensions for -1 and 2)

For an odd prime p,

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

Proof. The first part of the theorem follows directly from work above. Observe that this implies -1 is a quadratic residue if $p \equiv 1 \pmod 4$ and -1 is not a quadratic residue if $p \equiv 3 \pmod 4$. For the second part of the theorem, note that

$$\begin{aligned}
2^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)! = 2 \cdot 4 \cdot 6 \cdots p - 1 &= \prod_{k=1}^{\left\lfloor \frac{p-1}{4} \right\rfloor} (2k) \cdot \prod_{k=\left\lfloor \frac{p-1}{4} \right\rfloor + 1}^{\frac{p-1}{2}} (2k) \\
&\equiv \prod_{k=1}^{\left\lfloor \frac{p-1}{4} \right\rfloor} (2k) \cdot (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor} \prod_{k=1}^{\left\lfloor \frac{p+1}{4} \right\rfloor} (2k-1) \\
&\equiv (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor} \prod_{k=1}^{\frac{p-1}{2}} k \\
&\equiv (-1)^{\left\lfloor \frac{p-1}{2} \right\rfloor} \left(\frac{p-1}{2}\right)!.
\end{aligned}$$

Therefore,

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \equiv (-1)^{\left\lfloor \frac{p+1}{4} \right\rfloor}.$$

We can verify easily for all odd primes that $\left\lfloor \frac{p+1}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2$, so we are done. □

In particular, we see 2 is a quadratic residue when $p \equiv 1 \pmod 8$ or $p \equiv 7 \pmod 8$, and 2 is a quadratic nonresidue when $p \equiv 3 \pmod 8$ and $p \equiv 5 \pmod 8$.

With that said, let's move on to some basic examples.

Example 1.11

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 $S \pmod{1000}$.

Solution. Let $15a + 16b = x^2$ and $16a - 15b = y^2$. Since we have two equations with a and b, we can use these equations to solve for a and b in terms of x^2 and y^2. If we multiply the first equation by 16 and subtract 15 times the second equation, we get

$$481b = 16x^2 - 15y^2 \implies b = \frac{16x^2 - 15y^2}{481}.$$

Similarly, we get $a = \frac{15x^2+16y^2}{481}$. Note that $481 = 13 \cdot 37$. Therefore, since a is an integer,

$$15x^2 + 16y^2 \equiv 0 \pmod{13} \implies 2x^2 \equiv -3y^2 \pmod{13}$$

Multiplying both sides by $2^{-1} \equiv 7 \pmod{13}$, we see $x^2 = 5y^2 \pmod{13}$. If $13 \nmid y$, then we could write

$$\left(\frac{x}{y}\right)^2 = 5 \pmod{13}.$$

But from quadratic reciprocity,

$$\left(\frac{5}{13}\right)\left(\frac{13}{5}\right) = (-1)^{\frac{1}{4}\cdot 12 \cdot 4} = 1.$$

Since $\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$, 5 is a quadratic nonresidue mod 13, which contradicts the work above. Therefore, we must have $13 \mid y$. If that is true, we directly see that $13 \mid x$ as well.

Now, let's work mod 37. We know that $15x^2 + 16y^2 \equiv 0 \pmod{37}$. Therefore, $x^2 \equiv -16 \cdot 15^{-1} y^2 \pmod{37}$. Note that $15 \cdot 5 \equiv 1 \pmod{37}$, so $15^{-1} \equiv 5 \pmod{37}$. Therefore, we get $x^2 = -6y^2 \pmod{37}$.

Assume for the sake of contradiction that $37 \nmid y$. Then, it follows that -6 must be a quadratic residue mod 37. Since the Legendre symbol is multiplicative,

$$\left(\frac{-6}{37}\right) = \left(\frac{-1}{37}\right)\left(\frac{2}{37}\right)\left(\frac{3}{37}\right).$$

Since $37 \equiv 5 \pmod{8}$, 2 is a quadratic non residue and 1 is a quadratic residue. Also, by quadratic reciprocity,

$$\left(\frac{3}{37}\right)\left(\frac{37}{3}\right) = 1 \implies \left(\frac{3}{37}\right) = 1,$$

$$\left(\frac{6}{37}\right) = -1 \cdot \left(\frac{3}{37}\right) = -1 \cdot 1 = -1.$$

Therefore, we see 6 is not a quadratic residue, so we must have $37 \mid y$. This also implies $37 \mid x$.

Combing the above work, $481 \mid x$ and $481 \mid y$. Let $x = 481x_1$ and $y = 481y_1$. Then,

$$a = 481(15x_1^2 + 16y_1^2), \qquad b = 481(16x_1^2 - 15y_1^2).$$

We see that $a + b$ is minimized when $x_1 = y_1 = 1$. Therefore, we obtain $a + b = 481 \cdot 32 \equiv \boxed{392} \pmod{1000}$. □

Example 1.12 (Folklore)

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

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

Solution. Note that, for a fixed y, there is 1 solution for x if $y^2 = 1$, there are 2 if $1 - y^2$ is a nonzero quadratic residue, and there are 0 if it is a non quadratic residue (NQR). Letting $p = 2027$, it is easy to see that these values match with $\left(\frac{1-y^2}{p}\right) + 1$. So, the number of solutions is

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

Call the sum on the RHS S. Note that $y \to \frac{1}{y}$ is a bijection on $(\mathbb{Z}/2027\mathbb{Z})^\times$ (the nonzero residues mod 2027), so

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

By the definition of quadratic residue, the second term should always be 1, so

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

Now, since $p \equiv 3 \pmod 4$, we know that $\left(\frac{-1}{p}\right) = -1$. Hence, $S = -S \implies S = 0$. So, our answer is

$$2028 + S = \boxed{2028}$$

□

§1.1 Aside on the 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

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

In this case, $\left(\frac{a}{n}\right) = 0$ when $\gcd(a, n) \neq 1$. Also, $\left(\frac{a}{n}\right) = \left(\frac{b}{m}\right)$ when $a \equiv b \pmod n$.

For completeness, we will state the quadratic reciprocity theorem with Jacobi symbols.

Theorem 1.13 (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

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

Remark 1.14. It is important to note that $\left(\frac{a}{n}\right)$ 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. On the other hand, if $\left(\frac{a}{mn}\right) = -1$, then we *know* that a is a quadratic nonresidue mod mn.

Example 1.15 (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* $\left(\frac{a}{p}\right)$.

Solution. We claim the function is

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

We can easily check this with quadratic reciprocity using Jacobi symbols. Since $p = a^2+b^2$, we must have $p \equiv 1 \pmod 4$ since $0, 1$ are the only quadratic residues mod 4. When $a \equiv 1 \pmod 2$,

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right)(-1)^{\frac{1}{4}(a-1)(p-1)} = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = \left(\frac{b^2}{a}\right) = 1.$$

When $a \equiv 2 \pmod 4$, $a^2 \equiv 4 \pmod 8$ and $b^2 \equiv 1 \pmod 8$ (since b is odd), so $p \equiv 5 \pmod 8$. In this case 2 is not a quadratic residue mod p. Then, we have

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{\frac{a}{2}}{p}\right) = -1 \cdot \left(\frac{p}{\frac{a}{2}}\right) = -1 \cdot \left(\frac{a^2+b^2}{\frac{a}{2}}\right) = -1 \cdot \left(\frac{b^2}{\frac{a}{2}}\right) = -1.$$

When $a \equiv 0 \pmod 4$, let k be the maximal integer such that $2^k \mid a$. Let $a = 2^k a_1$. In this case $a^2 + b^2 \equiv 0 + 1 \equiv 1 \pmod 8$. This means that 2 is a quadratic residue modulo p. Then, since the Jacobi symbol is multiplicative,

$$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^k \left(\frac{a_1}{p}\right) = \left(\frac{a_1}{p}\right) = \left(\frac{p}{a_1}\right) = \left(\frac{2^{2k}a_1^2+b^2}{a_1}\right) = \left(\frac{b^2}{a_1}\right) = 1.$$

Therefore, our function works and we are done. □

§2 p-adic Valuations

Definition 2.1. Let p be a prime number and n be any positive integer. We define the *p-adic valuation* of n to be the largest nonnegative integer k such that n is divisible by p^k. This integer k is often written as $\nu_p(n)$.

For example, $\nu_2(96) = 5$ because 2^5 is the largest power of 2 that divides 96. There are some elementary properties of the p-aidc valuation that you should check:

- $\nu_p(a+b) \geq \min(\nu_p(a), \nu_p(b))$. (In fact, if $\nu_p(a) \neq \nu_p(b)$ then equality holds.)
- $\nu_p(ab) = \nu_p(a) + \nu_p(b)$

We discuss a couple of useful theorems regarding p-adic valuations:

Theorem 2.2 (Legendre's Formula)

For any prime p and positive integer n, $\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots$. (Note that the sum on the right-hand side is finite as eventually all terms are 0.)

Proof. Let's write $n! = 1 \cdot 2 \cdot 3 \cdots n$.

- All multiples of p in this product contribute a factor of p; there are $\left\lfloor \frac{n}{p} \right\rfloor$ of these multiples.
- All multiples of p^2 contribute an *additional* factor of p; there are $\left\lfloor \frac{n}{p^2} \right\rfloor$ of these.
- All multiples of p^3 contribute a *third* factor of p; there are $\left\lfloor \frac{n}{p^3} \right\rfloor$ of these.
- $\cdots$

Adding up all of these contributions of factors of p, we get

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

□

Theorem 2.3 (also Legendre's Formula)

$\nu_p(n!) = \frac{n - s_p(n)}{p-1}$ as well, where $s_p(n)$ is the sum of the digits of the base-p representation of n.

Proof. Let $n = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_1 p + a_0$ be the base-p representation of n. By Legendre's Formula

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

But we have

$$\begin{aligned}
\left\lfloor \frac{n}{p} \right\rfloor &= a_k p^{k-1} + a_{k-1} p^{k-2} + \cdots + a_2 p + a_1, \\
\left\lfloor \frac{n}{p^2} \right\rfloor &= a_k p^{k-2} + a_{k-1} p^{k-3} + \cdots + a_2, \\
&\cdots, \\
\left\lfloor \frac{n}{p^k} \right\rfloor &= a_k.
\end{aligned}$$

If we sum, we get

$$\begin{aligned}\nu_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots \\ &= a_k(p^{k-1} + p^{k-2} + \cdots + 1) + a_{k-1}(p^{k-2} + \cdots + 1) + \cdots + a_2(p+1) + a_1 \\ &= a_k \frac{p^k - 1}{p-1} + a_{k-1}\frac{p^{k-1}-1}{p-1} + \cdots + a_2 \frac{p^2-1}{p-1} + a_1 \frac{p-1}{p-1}.\end{aligned}$$

Now let's compare to $\frac{n - s_p(n)}{p-1}$. This is

$$\frac{1}{p-1}\left(a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0 - a_k - a_{k-1} - \cdots - a_0\right)$$

which works out to

$$\frac{a_k(p^k - 1) + a_{k-1}(p^{k-1} - 1) + \cdots + a_2(p^2 - 1) + a_1(p-1)}{p-1}$$

and this is is identical to the expression we found by summing $\left\lfloor \frac{n}{p^i} \right\rfloor$. So the two formulas are the same: $\nu_p(n!) = \frac{n - s_p(n)}{p-1}$. □

Theorem 2.4 (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

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

Proof. We will induct on $\nu_p(n)$. Our base case is $\nu_p(n) = 0$. We have to show that if $p \nmid n$, then $\nu_p(a^n - b^n) = \nu_p(a - b)$, or alternatively that p does not divide

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + \cdots + b^{n-1}.$$

Let's use the hypothesis $p|a - b$, from which we get $a \equiv b \pmod{p}$. Then modulo p, we have

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

We assumed that $p \nmid n$ for our base case, and $p \nmid a^{n-1}$ by assumption. So this is nonzero modulo p, so the base case is complete.

For the inductive step, suppose that our lemma holds whenever $\nu_p(n) = k$; we'll prove it for $\nu_p(n) = k + 1$. Suppose that $\nu_p(n) = k + 1$ and define $N = \frac{n}{p}$ (which is an integer); then $\nu_p(N) = k$. We wish to show

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

But $n = pN$ so this is equivalent to

$$\nu_p(a^{pN} - b^{pN}) = \nu_p(a - b) + \nu_p(N) + 1.$$

By the inductive hypothesis we have

$$\nu_p(a^N - b^N) = \nu_p(a - b) + \nu_p(N)$$

so subtracting the above two equations we see it suffices to show

$$\nu_p(a^{pN} - b^{pN}) = \nu_p(a^N - b^N) + 1$$

or equivalently that

$$\frac{a^{pN} - b^{pN}}{a^N - b^N}$$

is divisible by p but not p^2. This is what we'll prove.

Since p divides $a - b$, it also divides $a^N - b^N$. Let $b^N = M$ and $a^N = M + pk$ for some integer k. By hypothesis $p \nmid M$. Then

$$\frac{a^{pN} - b^{pN}}{a^N - b^N} = \frac{(M + pk)^p - M^p}{pk}.$$

Let's expand with the Binomial Theorem:

$$\frac{1}{pk}\left((M + pk)^p - M^p\right) = \binom{p}{1}M^{k-1} + \binom{p}{2}M^{p-1}pk + \binom{p}{3}M^{p-2}(pk)^2 + \cdots + (pk)^{p-1}.$$

(check this!). All terms on the right-hand side are divisible by p, so the expression is divisible by p. Now we have to check that it's not divisible by p^2. All terms after the second term are divisible by p^2 (they contain a factor of at least p^2). The second term is also divisible by p^2; it has a factor of p, and since p is odd (this is where we use this assumption!) p divides $\binom{p}{2}$ as well. Finally, the first term is not divisible by p^2; it has a factor of p, but $p \nmid M^{k-1}$. So the entire sum is divisible by p but not p^2, and we're done. □

Example 2.5 (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.

Solution. Since we want large prime powers dividing numbers of the form $149^n - 2^n$, we can use Lifting the Exponent. Let's try $\nu_3(149^n - 2^n)$ first. We see that 3 is an odd prime, $3|149 - 2$, and 3 does not divide either of 149 and 2. So Lifting the Exponent tells us that

$$\nu_3(149^n - 2^n) = \nu_3(149 - 2) + \nu_3(n) = \nu_3(n) + 1.$$

Thus in order for $149^n - 2^n$ to be divisible by 3^3 we need $\nu_3(n) + 1 \geq 3$, so $3^2|n$.

Similarly, we see that 7 is odd, $7|149 - 2$, and 7 does not divide either of 149 and 2, so

$$\nu_7(149^n - 2^n) = \nu_7(149 - 2) + \nu_7(n) = \nu_7(n) + 2.$$

In order for $149^n - 2^n$ to be divisible by 7^7 we need $\nu_7(n) + 2 \geq 7$, so $7^5 | n$.

Finally, we calculate $\nu_5(149^n - 2^n)$, but we run into a problem: we can't use Lifting the Exponent because $5 \nmid 149 - 2$. We have

$$149^n - 2^n \equiv 4^n - 2^n \equiv 2^n(2^n - 1) \pmod 5$$

so if $5|149^n - 2^n$ then we need $5|2^n - 1$ (as 5 can't divide 2^n). We can check that this occurs precisely when n is divisible by 4. Let $n = 4k$; we now use Lifting the Exponent in the following form:

$$\nu_5(149^{4k} - 2^{4k}) = \nu_5((149^4)^k - (2^4)^k)) = \nu_5(149^4 - 2^4) + \nu_5(k) = \nu_5(k) + 1$$

(check by hand that $\nu_5(149^4 - 2^4) = 1$). In order for 5^5 to divide $149^n - 2^n$, we thus need $\nu_5(k) + 1 \geq 5$, or $5^4 | k$ and thus $4 \cdot 5^4 | n$.

We now know that n must be divisible by 3^2, 7^5, and $4 \cdot 5^4$, so n must be divisible by their least common multiple,

$$2^2 \cdot 3^2 \cdot 5^4 \cdot 7^5.$$

Since n is a multiple of this number, it has at least as many factors. So the least possible number of factors of n is simply the number of factors of this number, which is

$$(2+1)(2+1)(4+1)(5+1) = \boxed{270}.$$

□

Example 2.6 (ISL 1991)

Find the greatest power of 1991 which divides

$$1990^{1991^{1992}} + 1992^{1991^{1990}}$$

Solution. We recognize this form as similar to that of *LTE*. The only problem is that 1991 is not prime, and we have a + instead of a −. Actually, we will see that none of these prove to be problems.

As $1991 = 11 \cdot 181$, it suffices to find the ν_{11} and ν_{181} of the expression. We will only show the former since the latter is analogous. What we want is to somehow apply LTE on

$$S = \left(1990^{1991^2}\right)^{1991^{1990}} + 1992^{1991^{1990}}$$

First, note that $1990^{1991^2} + 1992 \equiv 1 + (-1)^{\text{odd}} \equiv 0 \pmod{11}$, and neither base is divisible by 11. So, we are in the right setup to apply LTE. To deal with the +, note that both of the exponents are odd, so we can actually write our expression as

$$S = \left(1990^{1991^2}\right)^{1991^{1990}} - (-1992)^{1991^{1990}}$$

and now normal LTE gives that

$$\nu_{11}(S) = 1990 + \nu_{11}\left(1990^{1991^2} + 1992\right)$$

Unfortunately, we can no longer use LTE on the remaining expression. However, we can split it up as $\left(1990^{1991^2}+1\right)+1991$, and the former has ν_{11} of 3 by another application of LTE. As we are adding 1991, which has $\nu_{11}(1991)=1$, to a number divisible by 11^3, the resulting sum is a number with $\nu_{11}=1$. Hence,

$$\nu_{11}(S)=1990+\nu_{11}\left(1990^{1991^2}+1992\right)=1990+1=1991$$

The exact same logic holds for ν_{181}, so our answer is $\boxed{1991}$. □

Example 2.7 (IMO 2019/4)
Find all pairs (k,n) of positive integers such that

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

Solution. Let's first factor the right-hand side by pulling out as many powers of 2 out of each factor as we can: we get

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

From this we immediately see that $v_2(k!)=\frac{n(n-1)}{2}$. By Legendre,

$$v_2(k!)=\left\lfloor\frac{k}{2}\right\rfloor+\left\lfloor\frac{k}{4}\right\rfloor+\ldots\le\frac{k}{2}+\frac{k}{4}+\ldots=k.$$

This tells us that $k\ge\frac{n(n-1)}{2}$; in other words, k must be pretty large.

However, the presence of factors of the form 2^i-1 inspire us to try consider the ν_p of other primes. Let's try $p=3$. In this case, $3|2^i-1$ if and only if i is even. If $i=2j$, then by Lifting the Exponent

$$\nu_3(2^i-1)=\nu_3(4^j-1)=\nu_3(4-1)+\nu_3(j)=\nu_3(j)+1=\nu_3(i)+1.$$

Therefore for all i,

$$\nu_3(2^i-1)=\begin{cases}0 & i\text{ odd}\\ \nu_3(i)+1 & i\text{ even}\end{cases}$$

Using the same method as the proof of Legendre's Formula, we see that

$$\nu_3(2^{\frac{n(n-1)}{2}}(2^n-1)(2^{n-1}-1)\dots(2^1-1))=\left\lfloor\frac{n}{2}\right\rfloor+\left\lfloor\frac{n}{6}\right\rfloor+\left\lfloor\frac{n}{18}\right\rfloor+\cdots.$$

This is because in the product $(2^1-1)\cdots(2^n-1)$, each factor 2^i-1 with i a multiple of 2 provides a factor of 3, each i a multiple of 6 provides a second factor of 3, each i a multiple of 18 provides a third factor of 3, and so on. By Legendre we have

$$\nu_3(k!)=\left\lfloor\frac{k}{3}\right\rfloor+\left\lfloor\frac{k}{9}\right\rfloor+\cdots$$

so we have the equality

$$\left\lfloor\frac{k}{3}\right\rfloor+\left\lfloor\frac{k}{9}\right\rfloor+\cdots=\left\lfloor\frac{n}{2}\right\rfloor+\left\lfloor\frac{n}{6}\right\rfloor+\left\lfloor\frac{n}{18}\right\rfloor+\cdots.$$

This is pretty surprising; this tells us that k must be approximately proportional to n, while our earlier result gave us that k is at least a quadratic in n. So let's try to find an upper bound on k in terms of n; maybe we'll get a contradiction. We use the estimates

$$\left\lfloor \frac{n}{2} \right\rfloor + \left\lfloor \frac{n}{6} \right\rfloor + \left\lfloor \frac{n}{18} \right\rfloor + \cdots \leq \frac{n}{2} + \frac{n}{6} + \frac{n}{18} + \cdots = \frac{3}{4}n$$

and

$$\left\lfloor \frac{k}{3} \right\rfloor + \left\lfloor \frac{k}{9} \right\rfloor + \ldots > \left\lfloor \frac{k}{3} \right\rfloor > \frac{k}{3} - 1$$

This tells us that

$$\frac{3}{4}n > \frac{k}{3} - 1 \implies k < \frac{9}{4}n + 3.$$

But we know that $k \geq \frac{n(n-1)}{2}$; this implies

$$\frac{9}{4}n + 3 > \frac{n(n-1)}{2}.$$

This only holds for $n \leq 6$ (check this!) so now we only have to calculate possible solutions with $n \leq 6$.

- $n = 1$: Plugging in, we get $k! = 1$, and $k = 1$ works.
- $n = 2$: $k! = 6$, which has $k = 3$ as a solution.
- $n = 3$: $k! = 168$ which clearly has no solutions.
- $n = 4$: $k! = 2^6 \cdot 3^2 \cdot 5 \cdot 7$, which is impossible as $v_2(k!) \neq 6$ ($v_2(7!) = 4$ but $v_2(8!) = 7$).
- $n = 5$: $k! = 2^{10} \cdot 3^2 \cdot 5 \cdot 7 \cdot 31$, which is impossible as 31 divides $k!$ but not 29 (both 29 and 31 are prime).
- $n = 6$: $k! = 2^{15} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 31$, which is impossible as 31 divides $k!$ but not 29.

We conclude that $\boxed{(1,1) \text{ and } (3,2)}$ are the only solutions. □

§3 Problems

Problem 3.1 (2014 PUMaC NT #3)**.** Find the number of ending zeros of 2014! in base 9. Give your answer in base 9.

Problem 3.2 (2013 PUMaC NT #2)**.** What is the smallest positive integer n such that 2013^n ends in 001 (i.e. the rightmost three digits of 2013^n are 001?

Problem 3.3. Characterize all primes p which divide $x^2 - 3$ for some x.

Problem 3.4 (2013 PUMaC NT #8)**.** Find the number of primes p between 100 and 200 for which $x^{11} + y^{16} \equiv 2013 \pmod{p}$

Problem 3.5 (2012 PUMaC NT #6)**.** Let $p_1 = 2012$ and $p_n = 2012^{p_{n-1}}$ for $n > 1$. Find the largest integer k such that $p_{2012} - p_{2011}$ is divisible by 2011^k.

Problem 3.6. Show that 2 is a primitive root mod 3^k for any k.

Problem 3.7 (2019 OMO Fall #21)**.** Let p and q be prime numbers such that $(p-1)^{q-1}-1$ is a positive integer that divides $(2q)^{2p} - 1$. Compute the sum of all possible values of pq.

Problem 3.8. Let a, b be distinct reals such that $a^k - b^k$ is an integer for any $k \in \mathbb{N}$. Prove that a, b are both integers.

Problem 3.9 (Folklore)**.** Find the number of solutions to $x^2 + y^2 \equiv 1 \pmod{p}$ for fixed prime p.

Problem 3.10 (USOMO 2020/3)**.** Let p be an odd prime. An integer x is called a quadratic non-residue if p does not divide $x - t^2$ for any integer t.

Denote by A the set of all integers a such that $1 \le a < p$, and both a and $4 - a$ are quadratic non-residues. Calculate the remainder when the product of the elements of A is divided by p.

Problem 3.11 (USA TST 2014/2)**.** Let $a_1, a_2, a_3, \ldots$ be a sequence of integers, with the property that every consecutive group of a_i's averages to a perfect square. More precisely, for every positive integers n and k, the quantity

$$\frac{a_n + a_{n+1} + \cdots + a_{n+k-1}}{k}$$

is always the square of an integer. Prove that the sequence must be constant (all a_i are equal to the same perfect square).