Why are numbers beautiful? It’s like asking why is Beethoven’s Ninth Symphony beautiful. If you don’t see why, someone can’t tell you. I know numbers are beautiful. If they aren’t beautiful, nothing is.” Paul Erdős.

1. Basic concepts and results

- An integer $a$ is said to divide an integer $b$ if there exists an integer $c$ such that $b = ac$. In this case, we say that $a$ is a divisor of $b$.
- An integer $p > 1$ is prime if its only positive divisors are 1 and $p$. We call $p$ composite if $p$ is not prime.
- The greatest common divisor of two integers $a, b$ is the largest positive number $d$ so that $d$ divides $a$ and $b$, denoted by $\gcd(a, b)$.
- Two integers $a_1, a_2$ are said to be congruent modulo $b$ if $a_1 - a_2$ is divisible by $b$.
- Suppose that $a$ and $b$ are integers with $b \neq 0$. Then there exists unique integers $q$ and $r$ such that $0 \leq r < |b|$ and $a = bq + r$.
- Euclidean algorithm implies that for any two integers $a, b$, there exist integers $c$ and $d$ so that $\gcd(a, b) = ac + bd$.
- If $p$ is a prime and $p$ divides $ab$ then either $p$ divides $a$ or $p$ divides $b$.
- There are infinitely many prime numbers.
- The exponent of $p$ in the prime factorization of $n!$ is $\sum_{i=1}^{n} \left\lfloor \frac{n}{p^i} \right\rfloor$.
- Fermat’s little theorem is a special case of Euler’s theorem. It says $x^{p-1} = x \pmod{p}$ if $p$ is prime and $(p, x) = 1$.
- A linear equation $ax = b \pmod{n}$ has a solution if and only if $\gcd(a, n)$ divides $b$.
- For each natural number $n \geq 2$, the set $(\mathbb{Z}/n\mathbb{Z})^*$ of congruence classes $[x]$ of $n$ such that $\gcd(x, n) = 1$ is a group. The order of this group is denoted by $\varphi(n)$, called the Euler’s phi function.
- If $n = \prod p_i^{a_i}$, then $\varphi(n) = \prod p_i^{a_i-1}(p_i - 1)$.
- A function $f : \mathbb{N} \to \mathbb{C}$ is multiplicative if whenever $m, n \in \mathbb{N}$ and $\gcd(m, n) = 1$, we have $f(mn) = f(m)f(n)$.
- The Euler’s $\varphi$-function is multiplicative.
- The group $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic. In particular, there are $\varphi(\varphi(n))$ primitive roots modulo $n$.
- Fix a prime $p$. An integer $a$ not divisible by $p$ is a quadratic residue modulo $p$ if $a$ is a square modulo $p$; otherwise, $a$ is a quadratic nonresidue.
- Let $p$ be an odd prime and let $a$ be an integer. We call the following Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p|a \\ 1 & \text{if } a \text{ is a quadratic residue, and} \\ -1 & \text{if } a \text{ is a quadratic nonresidue.} \end{cases}$$

- Since there exist primitive roots modulo $p$, the subgroup of quadratic residues modulo $p$ has index two in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, there are exactly $\frac{p-1}{2}$ quadratic residues modulo $p$.

**Fundamental Theorem of Arithmetic.** Every natural number can be written as a product of primes uniquely up to order.

**Euler’s Theorem.** If $(x, n) = 1$, then $x^{\varphi(n)} = 1 \pmod{n}$.

**Wilson’s Theorem.** An integer $p > 1$ is prime if and only if $(p - 1)! = -1 \pmod{p}$.
Euler’s Lemma. Assume that $p$ is an odd prime. Then

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

Chinese Remainder Theorem. Let $n, m$ be relatively prime natural numbers. Then

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}. $$

Gauss’ Quadratic Reciprocity Law. Suppose $p$ and $q$ are distinct odd primes. Then

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

Also

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{8} \\ -1 & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases} $$

Dirichlet’s Theorem. Let $a$ and $b$ be integers with $\gcd(a, b) = 1$. Then there are infinitely many primes of the form $ax + b$.

Prime Number Theorem. (Gauss-Hadamard-Poussin) Let $\pi(x)$ be the number of primes less than $x$. Then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1. $$

2. Problems from Putnam exams

1972 A–5. Show that $n$ does not divide $2^n - 1$ for any $n > 1$.

**Hint.** Use Fermat’s little theorem.

1977 A–5. Show that for any prime $p$ and any natural numbers $m \geq n$, we have

$$\left(\frac{pm}{pn}\right) = \left(\frac{m}{n}\right) \pmod{p}. $$

**Hint.** The exponent of $p$ in $(pm)!$ is $m$ plus the exponent of $p$ in $m!$. Thus we may assume that both sides are not divisible by $p$. In this case, write $n = x_k p^k + x_{k-1} p^{k-1} + \cdots + x_1 p + x_0$ and $m-n = y_k p^l + \cdots + y_1 p + y_0$ then we must have $x_i + y_i < p$ for all $i$. Also, we can assume that $p > 2$. Using Wilson’s Theorem we deduce that

$$\frac{(pm)!}{p^{e(pm)}} = (-1)^m \frac{m!}{p^{e(m)}} $$

where $e(m)$ is the exponent of $p$ in $m!$. From that we get the result.

1985 A–4. Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3a_i$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many $a_i$?

**Hint.** Use Euler’s Theorem (answer is 87).

1989 A–1. How many primes among the positive integers, written as usual in base 10, are alternating 1’s and 0’s, beginning and ending with 1?

**Hint.** Only 101 is prime.

1992 A–3. For a given positive integer $m$, find all triples $(n, x, y)$ of positive integers, with $n$ relatively prime to $m$, which satisfy

$$(x^2 + y^2)^m = (xy)^n. $$

**Hint.** The only possible solution is $m = 2k$, $n = 2k + 1$ and $x = y = 2^k$.

1994 B–6. For any integer $n$, set

$$n_a = 101a - 100 \cdot 2^a. $$

Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.

**Hint.** Trivially $a+b = c+d \pmod{100}$ and $2a+2b = 2c+2d \pmod{101}$. By Fermat’s little theorem, $2a+b = 2c+d \pmod{101}$. Now show that $(2^n - 2^a)(2^n - 2^b) = 0 \pmod{101}$. This implies that $\{2^a, 2^b\} = \{2^c, 2^d\} \pmod{101}$. Finally, show that 2 is a primitive root of 101.
1996 A–5. If \( p \) is a prime number greater than 3 and \( k = \lfloor 2p/3 \rfloor \), prove that the sum

\[
\binom{p}{1} + \binom{p}{2} + \cdots + \binom{p}{k}
\]

of binomial coefficients is divisible by \( p^2 \).

**Hint.** First, note that each term is divisible by \( p \). Now, note that

\[
\binom{p}{i}/p = (-1)^{i-1}/i \pmod{p}.
\]

Thus the sum dividing \( p \) is congruent to

\[
1 + \cdots + \frac{1}{k} - 2 \left( \frac{1}{2} + \cdots + \frac{1}{2[k/2]} \right) = 1 + \cdots + \frac{1}{p-1} = 0 \pmod{p}.
\]

1997 B–5. Prove that for \( n \geq 2 \),

\[
\sum_{2^i \leq n} k \equiv \sum_{2^i \leq n / p} k \pmod{n}.
\]

**Hint.** Let \( a_i \) be the tower of exponents of 2 with \( i \) terms. Prove by induction on \( n \) the following

\[
a_m = a_{m-1} \pmod{n}
\]

for all \( m \geq n \). Use Euler’s Theorem.

1998 A–4. Let \( A_1 = 0 \) and \( A_2 = 1 \). For \( n > 2 \), the number \( A_n \) is defined by concatenating the decimal expansions of \( A_{n-1} \) and \( A_{n-2} \) from left to right. For example \( A_3 = A_2A_1 = 10 \), \( A_4 = A_3A_2 = 101 \), \( A_5 = A_4A_3 = 10110 \), and so forth. Determine all \( n \) such that 11 divides \( A_n \).

**Hint.** Use a criterion for a number to be divisible by 11. The answer is \( n = 1 \pmod{6} \).

2000 B–2. Prove that the expression

\[
gcd(m,n)/n \binom{n}{m}
\]

is an integer for all pairs of integers \( n \geq m \geq 1 \).

**Hint.** Use the fact that \( \gcd(m,n) = am + bn \) for some integers \( a, b \).

2001 A–5. Prove that there are unique positive integers \( a, n \) such that \( a^{n+1} - (a+1)^n = 2001 \).

**Hint.** First note that \( a | 2002 = 2 \cdot 7 \cdot 11 \cdot 13 \). Taking modulo 3, we deduce that \( a = 1 \pmod{3} \) and \( n \) must be even. Taking modulo \( a+1 \) gives \( a+1 \) divides 2002. Thus \( a = 13 \). Now solve \( 13^{n+1} - 14^n = 2001 \). Working modulo 8 gives \( n = 2 \) is the only solution.

2003 B–3. Show that for each positive integer \( n \),

\[
n! = \prod_{i=1}^{n} \text{lcm}\{1, 2, \ldots, [n/i]\}.
\]

**Hint.** The power of \( p \) dividing \( \text{lcm}(1, 2, \ldots, k) \) is \( m \) where \( p^m \leq k < p^{m+1} \). Thus the power of \( p \) dividing \( \text{lcm}(1, 2, \ldots, [n/i]) \) is \( m \) where \( p^m \leq n/i < p^{m+1} \), or \( n/p^{m+1} < i \leq n/p^m \). There are \( [n/p^m] - [n/p^{m+1}] \) such \( i \). So the total power of \( p \) is \( \sum m([n/p^m] - [n/p^{m+1}]) = \sum [n/p^m] \).

2010 A–4. Prove that for each positive integer \( n \), the number \( 10^{10^{10^n}} + 10^{10^n} + 10^n - 1 \) is not prime.

**Hint.** Write \( n = 2^m k \) and note that

\[
10^{2^m j} = (-1)^j \pmod{10^{2^m} + 1}.
\]

2011 B–6. Let \( p \) be an odd prime. Show that for at least \((p + 1)/2\) values of \( n \) in \( \{0, 1, 2, \ldots, p - 1\} \), \( \sum_{k=0}^{p-1} k!n^k \) is not divisible by \( p \).

**Hint.** By Wilson’s Theorem, it is equivalent to prove that

\[
g(x) = \sum_{k=0}^{p-1} \frac{x^k}{k!}
\]

has at most \((p - 1)/2\) roots in \( \mathbb{F}_p \). Let \( h(x) = x^p - x + g(x) \). Then show that if \( z \) is a root of \( g \) then it is a double root of \( h \).
3. Other problems

O1. Find all natural number \( n \) such that \( 2^{n-1} | n! \).

**Hint.** Use the formula for the exponent of 2 in \( n! \).

O2. Prove that the number

\[
\sum_{k=0}^{n} \binom{2n+1}{2k+1} 2^{3k}
\]

is not divisible by 5 for any integer \( n \geq 0 \). IMO 1974/3

**Hint.** Let \( x = \sqrt{8} \). Then \((1 + x)^{2n+1} = a + bx\) where \( b \) is the given sum. Thus \( 2^{2n+1} = 8b^2 - a^2 \). If \( b \) is a multiple of 5, taking modulo 5, we have \( a^2 = \pm 2 \pmod{5} \). But the later has no solution.

O3. Show that

\[
\left( \frac{2n}{n} \right) | \text{lcm}\{1, 2, ..., 2n\}
\]

for all positive integers \( n \).

**Hint.** Use the formula for exponent of a prime \( p \) in \( n! \).

O4. Let \( m \) and \( n \) be arbitrary non-negative integers. Prove that

\[
\frac{(2m)!(2n)!}{mn!(m+n)!}
\]

is an integer. IMO 1972/3

**Hint.** Let \( f(m,n) \) be the number given. There is a recursive relation among \( f(m,n) \). Another way is to use the formula for exponent of a prime \( p \) in \( n! \).

O5. Show that \( \binom{2n}{n} \) is divisible by \( n+1 \) for any \( n \geq 1 \).

**Hint.** Let \( n + 1 = p^k l \) where \((p,l) = 1\). Then use formula for exponent of a prime \( p \) in \( n! \).

O6. Let \( p \) be a prime number of the form \( 4k + 1 \). Show that

\[
\sum_{i=1}^{p-1} \left( \left\lfloor \frac{2i^2}{p} \right\rfloor - 2 \left\lfloor \frac{i^2}{p} \right\rfloor \right) = \frac{p-1}{2}.
\]

**Hint.** The sum is equal to the number of residue classes \( k \) such that the residue class of \( k^2 \) is in \( [(p+1)/2, p-1] \). Now using quadratic reciprocity law, we know that \(-1 = d^2 \pmod{p} \) for some \( d \). For any \( x \), exactly one residue class of \( x \) or \( dx \) has the desired property.

O7. Assume that

\[
\frac{1}{1} + \frac{1}{p} + \cdots + \frac{1}{p-1} = \frac{m}{n}
\]

then \( p^2 \) divides \( m \).

**Hint.** Group the terms so that we can divide by \( p \). Then reduce it to prove that sum of quadratic residues is divisible by \( p \).

O8. Find all prime \( p \) such that there exist integers \( m, x \) and \( y \) such that \( p^m = x^3 + y^3 \).

O9. Let \( m, n \) be positive integers such that \( m \leq \frac{n^2}{4} \) and every prime divisor of \( m \) is at most \( n \). Show that \( m \) divides \( n! \).

O10. Suppose that \( \varphi(5^m - 1) = 5^n - 1 \) for some positive integers \( m, n \). Show that gcd\((m, n) > 1 \).

**References**