NUMBER THEORY

2022 WINTER CAMP - DANIEL SPIVAK

Here are some helpful results to keep in mind:

(1) The Chinese Remainder Theorem: If $gcd(m, n) = 1$, for any integers p, q there is a unique $0 \leq r < mn$ with $r \equiv p \pmod{m}$ and $r \equiv q \pmod{n}$.
(2) Euler's totient function: The number of integers $1 \leq i \leq n$ with $gcd(i, n) = 1$ is $\varphi(n) := n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k})$, where $p_1, \ldots, p_k$ are the distinct prime divisors of n.
(3) Euler's theorem: If $gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.
(4) In case $n = p^k$ or $n = 2p^k$, we have the primitive root theorem: $\exists r : r^{\varphi(p)}$ is the smallest positive power of r congruent to 1 mod p.
(5) p-adic valuation: $v_p(n)$ is the number of times that a prime p divides n, so if $n = p^k m$ with $p \nmid m$, then $v_p(n) = k$.
(6) The lifting exponents lemma: If $v_p(a-b) > 0$, then $v_p(a^n - b^n) = v_p(a - b) + v_p(n)$, except when $p = 2$ and $v_p(a - b) = 1$.
(7) $v_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots$
(8) Wilson's theorem: If p is prime, then $(p - 1)! \equiv -1 \pmod{p}$.
(9) For a polynomial P with integer coefficients, $P(x + n) \equiv P(x) \pmod{n}$.
(10) Quadratic reciprocity: for odd integers p, q, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, and $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$.

And here are some helpful problems to solve:

(1) Compute:
   (a) $\left(\frac{27}{83}\right)$
   (b) $\left(\frac{29}{59}\right)$
   (c) $\left(\frac{30}{101}\right)$
   (d) $\left(\frac{2021}{37}\right)$
(2) Find the last three digits of $2021^{2022^{2023}}$.
(3) Find all integer solutions (if they exist) to:
   (a) $13x + 11y = 2$
   (b) $24x + 16y = 12$
   (c) $6x + 10y + 15z = 1$
(4) What is the smallest integer n with 3^n ending in 00001?
(5) Find all n with $n^2 \equiv 1 \pmod{1001}$.
(6) Show that there is no n with $\varphi(n) = 2022$.
(7) A Pythagorean triple (a, b, c) is a triplet of positive integers satisfying $a^2 + b^2 = c^2$, and is called primitive if $gcd(a, b) = 1$. Show that in this case, $gcd(a, c) = gcd(b, c) = 1$, and that there exist positive integers x and y with $\{a, b\} = \{x^2 - y^2, 2xy\}$ and $c = x^2 + y^2$.
(8) Find all integer solutions to $x^2 + xy - y^2 = 10x - 9$ (You may have to look up Pell's equation, or ask me about it).
(9) Prove that $n^{n^{n^n}} - n^{n^n}$ is divisible by 2022 for any positive integer n.
(10) Define a sequence by $a_1 = 1$, and $a_n = a_{n-1} + 2^{a_{n-1}}$ for $n > 1$. Show that $a_1, a_2, \ldots, a_{3^{2022}}$ are distinct mod 3^{2022}.
(11) (ISL 2008 #1) Let n be a positive integer and let p be a prime number. Prove that if a, b, c are integers (not necessarily positive) satisfying the equations $a^n + pb = b^n + pc = c^n + pa$, then $a = b = c$.
(12) (ISL 2015 #1) Let a and b be positive integers such that $a!b!$ is a multiple of $a! + b!$. Prove that $3a \geq 2b + 2$.
(13) (ISL 2008 #3) Let $a_0, a_1, a_2, \ldots$ be a sequence of positive integers such that the greatest common divisor of any two consecutive terms is greater than the preceding term; in symbols, $gcd(a_i, a_{i+1}) > a_{i1}$. Prove that $a_n \geq 2^n$ for all $n \geq 0$.

(14) (ISL 2014 #4) Let $n > 1$ be a given integer. Prove that infinitely many terms of the sequence $(a_k)_{k\geq 1}$, defined by $a_k = \lfloor \frac{n^k}{k} \rfloor$ are odd.

(15) (ISL 2008 #4) Let n be a positive integer. Show that the numbers $\binom{2^n-1}{0}, \binom{2^n-1}{1}, \binom{2^n-1}{2}, \ldots, \binom{2^n-1}{2^{n-1}-1}$ are congruent modulo 2^n to $1, 3, 5 \ldots, 2^n - 1$ in some order.

(16) (ISL 2012 #6) Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

(17) (ISL 2009 #7) Let a and b be distinct integers greater than 1. Prove that there exists a positive integer n such that $(a^n - 1)(b^n - 1)$ is not a perfect square.