NUMBER THEORY

2020 WINTER CAMP - DANIEL SPIVAK

Here are some helpful results to keep in mind:

(1) Every positive integer can be written as the product of prime numbers, unique up to rearranging (if you accept 1 as the product of no prime numbers).
(2) Every pair of integers have a greatest common divisor, divisible by all other common divisors.
(3) The greatest common divisor can be determined by the Euclidean algorithm.
(4) Bezout's lemma: For positive integers x, y there exist a, b such that $ax + by = gcd(x, y)$.
(5) 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 $r \equiv q \pmod n$.
(6) 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.
(7) Euler's theorem: If $gcd(a, n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod n$.
(8) The lifting exponents lemma: Suppose a prime p divides $a - b$ exactly $x > 0$ times, and divides n exactly y times. Then p divides $a^n - b^n$ exactly $x + y$ times, except when $p = 2$ and $x = 1$.
(9) Wilson's theorem: If p is prime, then $(p - 1)! \equiv -1 \pmod p$.
(10) Quadratic reciprocity: for odd primes p, q, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$, and $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 8$.
(11) For a polynomial P with integer coefficients, $P(x + n) \equiv P(x) \pmod n$.

And here are some helpful problems to solve:

(1) Show that for any $a, b \in \mathbb{N}$, $gcd(a, b)lcm(a, b) = ab$.
(2) (IMO 1959 #1) Prove that $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.
(3) is 30 a quadratic residue mod 37? 39? 77?
(4) Find the last two digits of $2021^{2022^{2023}}$.

(5) Find all integer solutions (if they exist) to:
   (a) $6x + 15y = 2$
   (b) $23x + 14y = 7$
   (c) $2x + 5y + 12z = 1$
(6) What is the smallest integer n with 11^n ending in 00001?
(7) Find all n with $n^2 \equiv 1 \pmod{1001}$.
(8) Show that there is no n with $\varphi(n) = 2020$.
(9) 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 $c = x^2 + y^2$.
(10) Prove Wilson's theorem: $(n - 1)! \equiv -1 \pmod{n} \iff n$ is prime.
(11) Find all positive integers n with $n|2^n - 1$.
(12) Let a_1 be a positive integer, and let $a_n = a_{n-1} + \lfloor\sqrt{a_{n-1}}\rfloor$ for $n > 1$. Show that a_n is a perfect square for some n.
(13) Find all primes p, q with $pq|(5^p - 2^p)(5^q - 2^q)$.
(14) (CMO 2012 # 2) For any positive integers n and k, let $L(n, k)$ be the least common multiple of the k consecutive integers $n, \ldots, n+k-1$. Show that for any integer b, there exist integers n and k such that $L(n, k) > bL(n + 1, k)$.
(15) (CMO 2016 # 3) Find all polynomials $P(x)$ with integer coefficients such that $P(P(n) + n)$ is a prime for infinitely many integers n.
(16) Let P be a non-constant polynomial. Show that as n ranges over the natural numbers, $P(n)$ is divisible by infinitely many different prime numbers.
(17) (IMO 2005 # 4) Determine all positive integers relatively prime to the sequence $a_n = 2^n + 3^n + 6^n - 1$.
(18) Let p be a prime number, and let $S = \{p-n^2 : n \in \mathbb{N}, p-n^2 > 1\}$. Show that S has two distinct elements with one dividing the other.
(19) Prove that $n^{n^{n^{n^{n^n}}}} - n^{n^{n^n}}$ is divisible by 2020 for any positive integer n.
(20) Define a sequence by $a_1 = 1$, and $a_n = a_{n-1} + 2^{a_{n-1}}$ for $n > 1$. Show that $a_1, a_2, \ldots, a_{3^{2020}}$ are distinct mod 3^{2020}.
(21) (IMO 2007 # 5) Let a and b be positive integers. Show that if $4ab - 1$ divides $(4a^2 - 1)^2$, then $a = b$.
(22) (IMO 2010 # 3) Find all functions $g : \mathbb{N} \to \mathbb{N}$ such that for all positive integers m, n, $(g(m) + n)(g(n) + m)$ is a perfect square.