Constructions and Existence Proofs

Andres Buritica Monroy

1 Existence Results

Number theory has quite a few results about the existence of a number satisfying certain properties that you should be aware of. We've already seen many of these:

- There are infinitely many primes.
- (Bezout's Identity) For any coprime integers a and b, there are integers x and y such that $ax + by = 1$.
- (Chinese Remainder Theorem) For any positive integers $a_1, \ldots, a_n$, and any pairwise coprime positive integers $b_1, \ldots, b_n$, there is exactly one residue $x \pmod{b_1 \ldots b_n}$ such that $x \equiv a_i \pmod{b_i}$ for each i.
- There exists a generator mod $p^k, 2p^k$ for any prime p and positive integer k.
- (Pell Equations) For any positive integer d, there are infinitely many pairs (x, y) of positive integers such that $x^2 - dy^2 = 1$.
- (Hensel's Lemma) If P is a polynomial with integer coefficients, and r and n are positive integers such that $n \mid P(r)$ but $\gcd(n, P'(r)) = 1$, then for any positive integer k there is a positive integer r_k such that $n^k \mid P(r_k)$.

The pigeonhole principle isn't strictly a number-theoretic result but is also often useful (see e.g. density arguments). Here are a few other results that may be helpful:

- (Dirichlet's Theorem) For any coprime positive integers a and b, there are infinitely many positive integers k such that $a + bk$ is prime.
- (Bertrand's Postulate) For any positive integer n, there is a prime in $(n, 2n]$.
- (Fermat's Christmas Theorem) Let p be prime. There are positive integers a and b such that $p = a^2 + b^2$ unless $p \equiv 3 \pmod 4$.
- (Schur's Theorem) For any polynomial p with integer coefficients, the set of primes that divide $p(x)$ for some x is infinite.
- (Zsigmondy's Theorem) If $a > b > 0$ are coprime integers, then for any integer $n \geq 3$ there is a prime number p that divides $a^n - b^n$ and does not divide $a^k - b^k$ for any positive integer $k < n$, unless $(a, b, n) = (2, 1, 6)$. The same holds for $a^n + b^n$ with the exception $2^3 + 1^3 = 9$.

2 Advice

You know the drill — get your hands dirty and try small cases. For many of these problems, there is some property of the construction you want to control. Remember properties like Fermat/Euler and Wilson that allow you to control stuff. CRT is especially useful because it allows you to combine a bunch of modular conditions into one. Most of the time Dirichlet then gives you a prime for free.

Sometimes you just have to try a bunch of stuff until something magically works.

3 Problems

1. Prove that if n is not a multiple of 4, then there are positive integers a and b such that $n \mid a^2 + b^2 + 1$.
2. Let $s(n)$ be the sum of the digits of n. Prove that for each positive integer k there exists a positive integer n such that $n + s(n)$ equals either k or $k + 1$.
3. Let a and b be positive integers. Prove that there are infinitely many positive integers n such that $n^b - 1 \nmid a^n + 1$.
4. Let a, b, c be pairwise coprime positive integers. Prove that there exist infinitely many triples x, y, z of distinct positive integers such that $x^a + y^b = z^c$.
5. Prove that there exists a positive integer divisible by 2^{2023} whose decimal representation does not contain any zeros.
6. Prove that there are infinitely many pairs a and b of perfect squares such that they have the same number of digits in decimal, and their concatenation is also a square.
7. Prove that there exist infinitely many positive integers n such that $n^2 + 1 \mid n!$.
8. For which positive integers r and s does there exist a positive integer n such that nr and ns have the same number of divisors?

4 Homework

1. Prove that there are infinitely many distinct pairs a, b of coprime integers such that $a > 1, b > 1$ and $a + b \mid a^b + b^a$.
2. Prove that for each positive integer k there exists an arithmetic sequence of k positive rational numbers such that when they are written in lowest terms, all numerators and denominators are pairwise distinct.
3. Prove that there exists a positive integer m such that the equation $\varphi(n) = m$ has at least 2023 solutions n.