1. **Diophantine equations.** Diophantine equations are equations in integers, e.g., \( x^n + y^n = z^n \).

Most problems involving Diophantine equations ask you to show that an equation has no *integer* solution, or that it has only the “obvious” solutions. Here are some common strategies to approach such problems:

- To prove the *non-existence* of a solution, use contradiction: Assume a solution exists and show that this leads to a contradiction.
- Simplify the equation by dividing out common factors on both sides.
- Consider parity (even/odd) or congruences to an appropriate modulus. If you can show that the left and right sides are always of opposite parity (i.e., one is even, the other one is odd), they can obviously not be equal. Similarly, if the left side is always congruent to 1 or 2 modulo 4, and the right side is always congruent to 3 modulo 4, the two sides can not be equal.

(a) Prove that a sum of two odd squares (i.e., squares of odd integers) can never be equal to a square of an integer.

**Solution:** Use congruences modulo 4: If \( x \) is odd, then \( x \equiv 1, 3 \mod 4 \), so \( x^2 \equiv 1^2, 3^2 \equiv 1 \mod 4 \). Hence the sum of two odd squares, say \( x^2 \) and \( y^2 \), satisfies \( x^2 + y^2 \equiv 1 + 1 = 2 \mod 4 \). On the other hand, for any integer \( z \), we have \( z^2 \equiv 0^2, 1^2, 2^2, 3^2 \equiv 0, 1 \mod 4 \). Hence \( z^2 \) and \( x^2 + y^2 \) (for \( x \) and \( y \) odd) have always different remainders modulo 4, so can never be equal.

(b) (2014 UI Mock Putnam Exam) Show that a positive integer whose decimal representation contains each of the digits 1, 2, 3, 4, 5, 6, 7 exactly 3 times and does not contain the digit 8 (but with no restrictions on the number of the digits 0 and 9) cannot be a perfect square (i.e., a square of an integer).

**Solution:** We use congruences modulo 9. Since an integer is congruent to its sum of digits modulo 9, the given number must be congruent to \( 3(1 + 2 + \cdots + 7) = 84 \equiv 3 \mod 9 \). On the other hand, the possible congruences of a perfect square modulo 9 are \( 0^2 \equiv 0, (\pm 1)^2 \equiv 1, (\pm 2)^2 \equiv 4, (\pm 3)^2 \equiv 0, \) and \( (\pm 4)^2 \equiv 7 \mod 9 \). Since \( 3 \mod 9 \) is not on this list, the given number cannot be a perfect square.

(c) Let \( a, b, c \) be odd integers. Show that the equation \( ax^2 + bx + c = 0 \) has no integer solution \( x \). (Hint: Do not use the quadratic formula...)

**Solution:** We argue by contradiction. Suppose the given equation has an integer solution \( x \). If \( x \) is even, then of the three terms \( ax^2, bx, c \), the first two are even and the third is odd, so their sum is odd and therefore cannot equal 0. If \( x \) is odd, then all three terms \( ax^2, bx, c \), are odd, so their sum is again odd therefore cannot equal 0. Thus, in either case we have arrived at a contradiction. Hence the equation has no integer solutions.

(d) Let \( a, b, c \) be odd integers. Show that the equation \( ax^2 + bx + c = 0 \) has no rational solution \( x \). (Hint: Convert the problem to one involving integer solutions.)
2. Primes and composite numbers: An integer \( n \geq 2 \) is called composite if there exist integers \( a, b \in \{2, 3, 4, \ldots \} \) such that \( n = ab \); it is called prime if it cannot be written in this form.

(a) (B1, Putnam 1988) Show that any composite integer is expressible as \( xy + xz + yz + 1 \) with positive integers \( x, y, z \).

(Hint: By definition, a composite number be written in the form \( n = ab \) with \( a, b \) integers \( \geq 2 \). Thus, the problem reduces to showing that such a product \( ab \) can always be written in the form \( xy + xz + yz + 1 \), with appropriate choices of \( x, y, z \).

Solution: By definition, a composite number is one that can be written in the form \( ab \) for some integers \( a, b \geq 2 \). Given such a representation, let \( x = a - 1, y = b - 1, z = 1 \). Then \( x, y, z \) are positive integers and \( xy + xz + yz + 1 = xy + x + y + 1 = (x + 1)(y + 1) = ab \), which is a representation of the desired form.

(b) (A1, Putnam 1989) Find all prime numbers in the sequence \( 101, 10101, 1010101, 101010101, \ldots \).

(Hint: Find a general formula for these numbers, then try to split this formula into two (nontrivial) integer factors.)

Solution: The first number, 101, is prime. We will show that the remaining numbers are all composite. Let \( a_n \) be the \( n \)-th term in this sequence. Then

\[
a_n = 1 + 100 + \cdots + 100^n = \frac{100^{n+1} - 1}{100 - 1} = \left( \frac{10^{n+1} - 1}{10 - 1} \right) \cdot \left( \frac{10^{n+1} + 1}{10 + 1} \right)
\]

If \( n \) is odd, then \( 10^{n+1} - 1 = 100^{(n+1)/2} - 1 \) is divisible by \( 100 - 1 \), so both factors in (1) are integers \( \geq 2 \) (since \( n \geq 2 \)). If \( n \) is even, then \( 10^{n+1} + 1 \) is divisible by \( 10 + 1 \) and \( 10^{n+1} - 1 \) is divisible by \( 10 - 1 \), so both factors in (2) are integers \( \geq 2 \). Thus, in either case, we have obtained a nontrivial factorization of \( a_n \), proving that \( a_n \) is composite for \( n \geq 2 \).

(c) Show that, for any base \( b \geq 2 \), the number \( (10101)_b \) (i.e., 10101 interpreted in base \( b \)) is composite.

(Hint: Let \( f(b) \) denote this number. Express \( f(b) \) as a polynomial in \( b \) and try to factor it.)

Solution: We have the following nontrivial factorization:

\[
f(b) = 1 + b^2 + b^4 = \frac{b^6 - 1}{b^2 - 1} = \frac{b^3 - 1}{b - 1} \cdot \frac{b^3 + 1}{b + 1} = (1 + b + b^2)(1 - b + b^2).
\]


(a) The missing digit in \( 2^{29} \): The number \( 2^{29} \) is known to consist of exactly 9 decimal digits, all of which are pairwise distinct. Thus, exactly one of the ten digits 0, 1, 2, \ldots, 9 is missing. Without using a calculator or brute force hand calculation, determine which digit is missing.

Solution: We use congruences modulo 9. Calculating \( 2^{29} \mod 9 \) directly, we get

\[
2^{29} = 2^{6 \cdot 4 + 5} = 1^4 \cdot 32 = 5 \mod 9.
\]
On the other hand, since a number is congruent to its sum of digits modulo 9, we also have

\[ 2^9 \equiv 0 + 1 + 2 + \cdots + 9 - x = 45 - x \equiv 9 - x, \]

where \( x \) denotes the missing digit. Comparing the two evaluations, we get \( x = 4 \).

(b) A famous Diophantine equation: Find all integer solutions to the equation \( x^2 = 2y^2 \).

(Hint: This is a disguised form of a very famous result, with a classical proof!)

Solution: Obviously, \((x, y) = (0, 0)\) is a solution, and for any other solution \((x, y)\), both \( x \) and \( y \) would have to be nonzero. We will show that there are no nonzero solutions. We argue by contradiction. Assume \( x, y \) are nonzero integers satisfying \((*)\). Since \( x^2 = (-x)^2 \), changing the sign of \( x \) or \( y \) does not affect the equation \((*)\), so we may assume \( x \) and \( y \) are both positive integers. Moreover, dividing out powers of 2, we may assume that \( x \) and \( y \) are not both even. (More formally, if \( 2^k \) is the highest power of 2 dividing both \( x \) and \( y \), setting \( x_1 = x/2^k \) and \( y_1 = y/2^k \), gives a pair of integers that are not both even, but still satisfy \((*)\).)

From \((*)\) we see that \( x^2 \) is even, so \( x \) must be even as well. Therefore \( x = 2z \) for some integer \( z \). Then, by \((*)\), \( (2z)^2 = 2y^2 \), and thus \( 2z^2 = y^2 \). This forces \( y^2 \), and hence \( y \), to be even. But this contradicts our assumption that \( x \) and \( y \) cannot both be even. Hence \((*)\) has no positive integer solutions.

Remark: The above argument is the standard proof of the irrationality of \( \sqrt{2} \). If \( \sqrt{2} \) were rational, then \( \sqrt{2} = x/y \) with \( x \) and \( y \) (nonzero) integers, so we would get a nonzero solution to the given equation, \((*)\) \( x^2 = 2y^2 \).

(c) Primality of polynomial values. Let \( P(x) = \sum_{k=0}^{n} a_k x^k \) be a polynomial of degree \( n \geq 1 \) with integer coefficients. Show that there exist infinitely many positive integers \( n \) such that \( |P(n)| \) is composite.

Solution: Since \( P(x) \) has degree at least 1, we have \( |P(n)| \to \infty \) as \( n \to \infty \). Thus, there exists a positive integer \( n_0 \) such that \( P_0 = |P(n_0)| \geq 2 \). Since \( P(n) \) has integer coefficients, \( P_0 \) is a positive integer.

Now consider congruences modulo \( P_0 \). By the properties of congruences, we have

\[ n \equiv n_0 \mod P_0 \implies P(n) \equiv P(n_0) = P_0 \equiv 0 \mod P_0. \]

Hence \( P_0 \) divides \( P(n) \) for any \( n \) satisfying \( n \equiv n_0 \mod P_0 \), and if \( n \) is large enough, then we also have \( |P(n)| > P_0 \geq 2 \). Thus, \( |P(n)| \) is composite for any large enough \( n \) that is congruent to \( n_0 \) modulo \( P_0 \).

Challenge Problem of the Week

(B5, Putnam 1997) Let

\[ a_n = \underbrace{2^{2^{\cdots^2}}}_n \]

denote a “tower” of \( n \) 2’s, with the order of the exponentiations from top to bottom. Thus, \( a_1 = 2, a_2 = 2^2 = 4, a_3 = 2^4 = 16, \) etc. Prove that, for any integer \( m \geq 2 \), the sequence \( a_n \mod m, n = 1, 2, 3, \ldots, \) eventually becomes constant.

Solution: We will prove the assertion by induction on \( m \). For \( m = 2 \) all terms \( a_n \) are congruent to 0 mod 2, so the assertion holds trivially.

Now let \( m \geq 2 \) be given and suppose the assertion has been proved for all moduli \( \ell \leq m \). We seek to show that the assertion also holds for \( m + 1 \), i.e., that \( a_{n+1} \equiv a_n \mod m + 1 \) holds for all sufficiently large \( n \). Since \( a_n \) satisfies the recurrence \( a_{n+1} = 2^{a_n} \), it is enough to show that

\[ 2^{a_{n+1}} \equiv 2^{a_n} \mod m + 1 \]

(1)
holds for all sufficiently large \( n \).

If \( m + 1 \) is odd, then by the Euler-Fermat theorem, we have \( 2^a \equiv 2^b \mod m + 1 \) whenever \( a \equiv b \mod \phi(m + 1) \), where \( \phi(m) \) is the Euler Phi function. Thus, (1) is implied by

\[
a_{n+1} \equiv a_n \mod \phi(m + 1).
\]

Since \( \phi(m + 1) \leq m \), the induction hypothesis shows that (2), and hence also (1), holds for all sufficiently large \( n \), thus proving the induction step in the case \( m + 1 \) is odd.

If \( m + 1 \) is even, we can write \( m + 1 = 2^k p \), where \( k \) is a positive integer and \( p \) is odd. If \( p = 1 \), then \( m + 1 = 2^k \) and (1) holds trivially for all sufficiently large \( n \). Otherwise, we have \( 3 \leq p \leq m + 1 \), and thus \( 2 \leq \phi(p) < m + 1 \), and applying the induction hypothesis again we get, for all sufficiently large \( n \),

\[
a_{n+1} \equiv a_n \mod \phi(p).
\]

By the Euler-Fermat theorem, this implies

\[
2^{a_{n+1}} \equiv 2^{a_n} \mod p,
\]

and since we trivially have \( 2^{a_{n+1}} \equiv 2^{a_n} \mod 2^k \) for all sufficiently large \( n \), it follows that the latter congruence in fact holds with modulus \( 2^k p = m + 1 \). Thus we have again obtained (1) for sufficiently large \( n \), proving the induction step in the case when \( m + 1 \) is even, and completing the induction proof.

Happy Problemsolving!