Number Theory and Modular Arithmetic Problems

1. Suppose a prime number $p > 2$ is the sum of two squares. Show that $p-1$ is divisible by four.

   Solution. An even number squared is divisible by 4. An odd number squared has remainder 1 when divided by 4, since $(2k+1)^2 = 4k^2+4k+1$. Alternately, one says that 0 and 1 are the only squares mod 4. If p is the sum of two squares, p has remainder 0, 1, or 2 after division by 4. But p is odd, so p must have remainder 1 after division by 4, or $p-1$ is divisible by 4. $\square$

2. Determine all integral solutions of $a^2+b^2+c^2 = a^2b^2$. (Hint: Work modulo 4).

   Solution. The only solution is $a = b = c = 0$. Modulo 4, squares are either 0 or 1. Then a^2b^2 is 0 or 1 (mod 4). If $a^2b^2 \equiv 1 \pmod 4$ then $a^2 \equiv 1 \pmod 4$ and $b^2 \equiv 1 \pmod 4$, so that $a^2 + b^2 + c^2 \pmod 4$ is either 2 or 3, and cannot equal a^2b^2. Thus a, b, and c must all be even.

   Now suppose $a = 2a_1$, $b = 2b_1$, and $c = 2c_2$ are all even. Then $4a_1^2 + 4b_1^2 + 4c_1^2 = 16a_1^2b_1^2$, so that $a_1^2 + b_1^2 + c_1^2 = 4a_1^2b_1^2$. Then $a_1^2 + b_1^2 + c_1^2 \equiv 0 \pmod 4$, so that $a_1 = 2a_2$, $b_1 = 2b_2$, and $c_1 = 2c_2$ are all even. We then get $a_2^2 + b_2^2 + c_2^2 = 16a_2b_2$, and a_2, b_2, c_2 must be even as well. Repeat this process n times to produce $a = 2^na_n$, $b = 2^nb_n$, $c = 2^nc_n$ for any n. Since n is arbitrary, this is only possible if a, b, and c are all zero. $\square$

3. Prove that for any set of n integers, there is a subset of them whose sum is divisible by n.

   Solution. Let the numbers be $a_1, a_2, \ldots, a_n$. Form $S_1 = a_1$, $S_2 = a_1 + a_2$, up to $S_n = a_1 + a_2 + \cdots + a_n$. If one of the $S_k \equiv 0 \pmod n$ then S_k is divisible by n and the problem is soved. If not, then the $S_1, \ldots, S_n$ are n numbers, each in one of the $n-1$ non-zero equivalence classes modulo n. By the pigeonhole principle, two of these are the same, say $S_i \equiv S_j \pmod n$ and assume $i < j$ (without loss of generality). Then $S_j - S_i \equiv 0 \pmod n$, so n divides $a_{i+1} + \cdots + a_j$ and the problem is solved. $\square$

4. Suppose $f(x)$ is a polynomial with integral coefficients, and none of the integers $f(1), f(2), \ldots, f(2007)$ is divisible by 2007. Prove that f has no integral zero.

   Solution. Since f has integer coefficients, if $a \equiv b \pmod{2007}$, then $f(a) \equiv f(b) \pmod{2007}$. Suppose f has an integral zero, say $f(n) = 0$. Then there is an integer $1 \leq m \leq 2007$ with $n \equiv m \pmod{2007}$. Then $0 = f(n) \equiv f(m) \pmod{2007}$, so that $f(m)$ is divisible by 2007, a contradiction. Thus f has no integral zero. $\square$

5. A *lattice point* is a point whose coordinates are both integers. If a and b and chosen randomly from $1, 2, \ldots, 100$. What is the probability that the segment from $(0, a)$ to $(b, 0)$ contains an even number of lattice points?

   Solution. The line joining $(0, a)$ to $(b, 0)$ is $y = -\frac{a}{b}x + a$. If $(x, -\frac{a}{b}x + a)$ is a lattice point, then so is $(b - x, -\frac{a}{b}(b - x) + a) = (b - x, \frac{a}{b}x)$. So lattice points on the segment from $(0, a)$ to $(b, 0)$ occur in pairs, with the possible exception of the point $(\frac{b}{2}, \frac{a}{2})$. The segment from $(0, a)$ to $(b, 0)$ contains an odd number of lattice points if and only if $(\frac{b}{2}, \frac{a}{2})$ is a lattice point, which occurs if and only if both a and b are even. So, the probability of an odd number of lattice points is $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$, and the probability that the segment contains an even number of lattice points is $\frac{3}{4}$. □

6. Find the largest integer that is equal to the product of its digits.

   Solution. If the number n has $k > 1$ digits, and the leftmost digit is a, then $n \geq a \cdot 10^{k-1}$. Since the $k - 1$ rightmost digits are all less than 10, their product is strictly less than 10^{k-1}, so n is larger than the product of its digits. Thus, only single digit numbers can equal the product of their digits, and the largest such number is 9. □

7. Imagine you are at a school that has 100 lockers, all shut. Suppose the first student goes along the row and opens every locker. The second student then goes along and shuts every other locker beginning with locker number 2. The third student changes the state of every third locker beginning with locker number 3. (If the locker is open the student shuts it, and if the locker is closed the student opens it.) The fourth student changes the state of every fourth locker beginning with number 4. Imagine that this continues until the 100 students have followed the pattern with the 100 lockers. At the end, which lockers will be open and which will be closed?

   Solution. Locker n is changed for every divisor of n. If k divides n then n/k also divides n, so unless $k = n/k$, the divisors of n occur in pairs. If $k = n/k$ then $n = k^2$. So, if n is a square, it has an odd number of divisors and the locker will be open. If n is not a square, it has an even number of divisors and the locker will be closed. Thus all lockers are closed except $1, 4, 9, 16, 25, 36, 49, 64, 81, 100$, which are open. □

8. Do there exist 100 consecutive integers so that each is divisible by a perfect cube bigger than 1?

9. Show that the sequence $11, 111, 1111, 11111, \ldots$ contains no perfect squares.

   Solution. Since $100 \equiv 0 \pmod 4$, any of these numbers is equivalent to $11 \pmod 4$, and so is equivalent to $3 \pmod 4$. However, since $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 0$, and $3^2 \equiv 1 \pmod 4$, there are no squares equivalent to $3 \pmod 4$. None of the numbers in the sequence are perfect squares. □

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

Solution. Just by taking powers of 3 (mod 100), it is easy to see that $3^{20} \equiv 1 \pmod{100}$, and so $3^{3^4} = 3^{81} = 3 \cdot 3^{20} 3^{20} 3^{20} 3^{20} \equiv 3 \pmod{100}$. Now for any $x \geq 4$,

$$3^{3^x} = (3^{3^4})^{3^{x-4}} \equiv 3^{3^{x-4}} \pmod{100}$$

Repeatedly applying this,

$$3^{3^{3^3}} = 3^{3^{27}} \equiv 3^{3^3} \pmod{100}$$

A simple induction proof now shows that for any tower of exponents,

$$3^{3^{\cdot^{\cdot^{\cdot^{3}}}}} \equiv 3^{3^3} \pmod{100}$$

So, for $n \geq 3$,

$$a_n \equiv 3^{3^3} \equiv 3^7 3^{20} \equiv 3^7 \equiv 87 \pmod{100}$$

and 87 is the only number that occurs as the last two digits of a_n for $n \geq 3$. $\square$