TJUSAMO 2011 – Number Theory 1

Mitchell Lee and Andre Kessler

1 Problems from last week

1. Prove that every positive rational number can be written in the form $a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \frac{1}{a_n}}}$, for some positive integers n and $a_1, a_2, \cdots, a_n$.
2. In an $n \times n$ grid of numbers from $\{-1, 1\}$, there is one -1 in each row and each column. It is permitted to negate all the numbers in any given row or column. Find the minimum possible number of -1's in a grid which can be reached by these operations.
3. n lines, no two parallel and no three concurrent, are drawn in a plane. They split the plane into regions, each containing a number. One of the regions contains the number 1, and the others contain the number 0. It is permitted to simultaneously increment the numbers in any two adjacent (that is, sharing a common side) regions by 1. When is it possible to get all the numbers to be simultaneously divisible by 3?

2 Modular Arithmetic

Hello. Today, we will talk about number theory. Specifically, we will talk about modular arithmetic.

3 Introduction

We say that $a \equiv b \pmod{n}$ (read: a is congruent to b mod n) iff $a-b$ is a multiple of n. This relation is reflexive, symmetric, and transitive, which means it partitions the integers into equivalence classes; that is, the set of integers can be split into parts such that any two elements from the same part are equal and no two elements from different parts are equal. We call these parts *residue classes mod n*.

The nice thing about residue classes is that for any two residue classes A, B mod n, the sumset $A + B = \{a + b : a \in A, b \in B\}$ is also a residue class mod n. This is equivalent to the fact that if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then $a + b \equiv c + d \pmod{n}$. Additionally, the productset $AB = \{ab : a \in A, b \in B\}$ is a subset of a residue class mod n.

4 Division

Notice that the above two results do *not* imply that if $ac \equiv bc \pmod{n}$, then $a \equiv b \pmod{n}$. In fact, unfortunately this statement is false - $2 \cdot 3 \equiv 6 \cdot 3 \pmod{6}$, yet it is not the case that $2 \equiv 6 \pmod{6}$.

For $ac \equiv bc \pmod{n}$ to imply $a \equiv b \pmod{n}$, we only need c to have an inverse mod n - that is, a number c^{-1} with $cc^{-1} \equiv 1 \pmod{n}$. It is sufficient for c to share no common factor with n besides 1.

5 The Chinese Remainder Theorem

The Chinese Remainder Theorem states that if m, n are relatively prime positive integers, then the system $x \equiv a \pmod{m}$; $x \equiv b \pmod{n}$ has a unique solution mod mn. This is essentially a consequence of the existence of m^{-1} mod n.

6 Prime Moduli

Since every integer not divisible by a prime is relatively prime to it, every n not divisible by a prime p has an inverse mod p. In fact, it is even possible to assign residue classes mod p to any rational number with denominator not divisible by p: we set $\frac{a}{b}$ to be in the same residue class as ab^{-1}. The sumset of two residue classes will still be residue class, and the productset of two residue classes will still be a residue class.

Keep in mind *Fermat's Little Theorem*: that $a^{p-1} \equiv 1 \pmod{p}$ for any integers a, p with p prime and a not divisible by p. (This also implies $a^{p-2} \equiv a^{-1} \pmod{p}$.)

7 Composite Moduli

Most importantly, composite moduli can be "reduced" into prime-power moduli using the Chinese Remainder Theorem.

Also, Euler's Theorem states that $a^{\varphi(n)} \equiv 1 \pmod{n}$ for any relatively prime positive integers a, n, where $\varphi(n)$ is the number of positive integers less than or equal to n and relatively prime to n.

8 Small Moduli

To prove that a solution does not exist for a particular equation, it is sufficient to prove that there is no solution mod 2. Or mod 3. Or mod 8. Specifically, you might use the fact that 0, 1, and 4 are the only squares mod 8.

9 Problems

1. Prove Fermat's Little Theorem.

2. Prove Euler's Theorem.

3. Prove that $(p-1)! \equiv -1 \pmod{p}$ for all primes p.

4. Prove that the sum of the squares of 3, 4, 5, or 6 consecutive integers is not a perfect square.

5. A set $a_1, a_2, \cdots, a_n$ is called a complete residue class mod n if no two of the elements are equivalent mod n. $a_1, a_2, \cdots, a_n$ and $b_1, b_2, \cdots, b_n$ are complete residue classes mod n. For which n is it possible that $a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n$ is a complete residue class mod n? For which n is it possible that $a_1b_1, a_2b_2, \cdots, a_nb_n$ is a complete residue class mod n?

6. Let p be a prime, and let k be a positive integer relatively prime to $p-1$. If a is an integer with $a^k \equiv 1 \pmod{p}$, prove that $a \equiv 1 \pmod{p}$.

7. If a and b are positive integers with $a \equiv b \pmod{n}$, show that $a^n \equiv b^n \pmod{n^2}$.

8. Show that if n is a fixed positive integer, then $2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \cdots$ eventually becomes constant mod n.

9. Prove that for all positive integers $a > 1$ and n, n is a divisor of $\varphi(a^n - 1)$.

10. Find all integers n such that n is a factor of $2^n - 1$.

11. Find all integers n such that n^2 is a factor of $2^n + 1$.