Divisibility

Ben Kang, Holden Mui, Mark Saengrungkongka

Name: ______________________________

Date: _______________________________

Divisibility is an important topic in olympiad number theory. An integer n is *divisible* by an integer k if n is a multiple of k.

For any two integers a and b, the *greatest common divisor* of a and b is the largest divisor of both a and b. This greatest common divisor is denoted $\gcd(a, b)$. For any positive integer k, k divides $\gcd(a, b)$ if k divides both a and b.

Problem 1 (Euclidean Algorithm).

(a) Prove that $\gcd(a - b, b) = \gcd(a, b)$ for any positive integers a and b.

(b) Prove that $\gcd(a - kb, b) = \gcd(a, b)$ for any positive integers a, b, and k.

Problem 2. Compute:

(a) $\gcd(24, 60)$

(b) $\gcd(270, 192)$

(c) $\gcd(1971, 10001)$

Problem 3.

(a) Prove that $\frac{21n+4}{14n+3}$ is an irreducible fraction for all positive integers n.

(b) Prove that $\gcd(n+1, n^2-7) < 8$ for every positive integer n.

(c) Prove that $\gcd(n^2+1, n^3+1)$ is 1 or 2 for every positive integer n.

All positive integers can be classified into the following three types.

- A *prime number* is a positive integer greater than 1 that has no divisor other 1 and itself. The first ten prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, and 29.
- A *composite number* is a positive integer that is a product of two smaller positive integers. The first ten composite numbers are 4, 6, 8, 9, 10, 12, 14, 15, 16, and 18.
- 1 is neither prime nor composite.

The following facts about prime numbers are true but not easy to prove.

- Let p be a prime number and a and b be any integers. If p divides ab, then p divides a or p divides b.
- Every positive integer can be uniquely expressed as an unordered product of prime numbers.

Problem 4.

(a) Prove that there are infinitely many prime numbers.

(b) Prove that there are infinitely many prime numbers congruent to 3 modulo 4.

Problem 5 (Fermat's Little Theorem). Let p be a prime number, and let a be a positive integer not divisible by p.

(a) Prove that $a, 2a, 3a, \ldots, (p-1)a$ are distinct modulo p.

(b) Prove that $a^{p-1} \equiv 1 \pmod{p}$.

Problem 6.

(a) Let $p \equiv 3 \pmod{4}$ be a prime. Prove that if p divides $a^2 + b^2$, then p divides both a and b.

(b) Is $2021 = 43 \cdot 47$ a sum of two squares?