Number Theory

Anthony Erb Lugo
(tonypr@google.com)

November 2020

1 Modular Arithmetic

1.1 Notation

We say $a \equiv b \pmod{n}$ for $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n > 1$ if $n | a - b$. That is, a is congruent to b modulo n if n divides $a - b$. Ex. $7 \equiv 2 \pmod{5}$.

1.2 Theorems

Theorem 1.1 (Wilson's Theorem)**:** Given a prime p, the following holds:

$$(p-1)! \equiv -1 \pmod{p}.$$

Theorem 1.2 (Fermat's Little Theorem)**:** Let a be a positive integer and let p be a prime. Then

$$a^p \equiv a \pmod{p}.$$

1.3 Warm-up Problems

1. What are the possible values of $x^2 \pmod{5}$ for positive integers x?
2. Consider the following arithmetic sequence $2, 6, 10, 14, \cdots$. Show that this sequence contains no perfect squares.
3. Calculate $21! \pmod{23}$.

1.4 Examples

Example 1.3: Let $S(n)$ be the sum of the digits of n. Show that $n \equiv S(n) \pmod{9}$.
Example 1.4: Let p be an odd prime, show that:

$$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}.$$

Example 1.5: Let p be a prime number, show that:

$$1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}.$$

Example 1.6: Let p be a prime. Prove that p divides $ab^p - ba^p$ for all integers a, b.

Example 1.7: Let a, b be positive integers and p a prime number. Show that if $p|a^p - b^p$, then $p^2|a^p - b^p$.

Example 1.8: Let a, b be positive integers and n an odd positive integer. Prove that $a + b|a^n + b^n$.

Example 1.9: Let $a, b > 1$ be positive integers. Prove that $2^a - 1|2^{ab} - 1$.

2 Divisibility

Theorem 2.1 (The Fundamental Theorem of Arithmetic)**:** Every integer greater than 1 can be written uniquely as

$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

where each p_i is a distinct prime and the e_i are positive integers.

Lemma 2.2 (Euclid's Lemma)**:** If p is a prime, $p|ab \implies p|a$ or $p|b$.

2.1 Useful Formulas

1. If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n, then n has $(e_1+1)\cdots(e_k+1)$ positive divisors.

2. If $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n, then the sum of the divisors of n is:

$$\sum_{d|n}^{n} d = \prod_{i=1}^{k}(1 + p_i + p_i^2 + \cdots + p_i^k) = \prod_{i=1}^{k} \frac{p_i^{k+1} - 1}{p_i - 1}.$$

3. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$.

4. $x, y \in \mathbb{Z}$, $x|y \implies |x| \leq |y|$.

2.2 Warm-up Problems

1. How many factors does 2020 have?

2. Show that 6 divides $n^3 + 5n$ for all positive integers n.

2.3 Examples

Example 2.3: Prove that if n isn't prime, then $2^n - 1$ is also not prime.

Example 2.4: Let $P(x)$ be a polynomial with integer coefficients. Show that for any distinct integers a, b, we have $a - b|P(a) - P(b)$.

Example 2.5: Show that there doesn't exist a polynomial $P(x)$ with integer coefficients such that $P(2024) = 11$ and $P(2020) = 9$.

Example 2.6: Let $a_1, a_2, \cdots a_n$ be integers in the set $\{-1, 1\}$ such that

$$a_1a_2 + a_2a_3 + \cdots + a_{n-1}a_n + a_na_1 = 0.$$

Prove that 4 divides n.

Example 2.7: (USAMO, 1974) Let a, b and c denote three distinct integers, and lt P denote a polynomial having all integer coefficients. Show that it is impossible that $P(a) = b$, $P(b) = c$, and $P(c) = a$.