Varsity: Modular Arithmetic

Varsity: Annie Xu

1 Definitions/Review

- An integer p is called prime if when p divides a product ab (where a, b are integers), then p divides a or p divides b. Equivalently, p is prime if $p = ab$ (where a, b are integers) implies that either $a = 1$ or $b = 1$.

  Note that this may be slightly different from the usual definition of being divisible by only 1 and itself. These definitions are essentially equivalent for all contexts which you will encounter, but are not actually the same in all contexts.

- Given integers a, b, c where $b \neq 0$, we write $a \equiv c \pmod{b}$ if b divides $(a - c)$.

- The Fundamental Theorem of Arithmetic states that every nonzero integer can be written uniquely (up to order) as a product of primes.

2 Warm-Up Problems

1. Determine if the following implications are true or false:
   (a) If $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$
   (b) If $a \equiv b \pmod{m}$ then $ac \equiv bc \pmod{m}$
   (c) If $ac \equiv bc \pmod{m}$ then $a \equiv b \pmod{m}$
   (d) If $ab \equiv 0 \pmod{m}$ then $a \equiv 0 \pmod{m}$ or $b \equiv 0 \pmod{m}$
   (e) If $ac \equiv bc \pmod{mc}$ then $a \equiv b \pmod{m}$

   What happens if m is prime and c is not a multiple of m?

2. (PUMaC 2009) If $17! = 355687ab8096000$, where a, b are two missing digits, find a and b.

3. We define the Fibonacci numbers by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$. Compute $gcd(F_{100}, F_{99})$ and $gcd(F_{100}, F_{95})$.

4. Prove that if $a \equiv b \pmod{n}$, then for all positive integers e that divide both a and b,

$$\frac{a}{e} \equiv \frac{b}{e} \pmod{\frac{n}{gcd(n, e)}}$$

3 Problems

1. When 30! is computed, it ends in 7 zeros. Find the digit that immediately precedes these zeros.

2. (AHSME 1960) Let m and n be any two odd numbers, with n less than m. What is the largest integer which divides all possible numbers of the form $m^2 - n^2$?

3. (2002 Indonesia MO) Show that $n^4 - n^2$ is divisible by 12 for any integers $n > 1$.
4. (AIME 1984) The integer n is the smallest positive multiple of 15 such that every digit of n is either 8 or 0. Compute $\frac{n}{15}$.
5. (2008 Mock ARML) Given that the sum of all positive integers with exactly two proper divisors, each of which is less than 30, is 2397, find the sum of all positive integers with exactly three proper divisors, each of which is less than 30 (a proper divisor of n is a positive integer that divides but is not equal to n).
6. (Canadian MO 1971) Let n be a five digit number (whose first digit is non-zero) and let m be the four digit number formed from n by removing its middle digit. Determine all n such that n/m is an integer.
7. (USAMO 1972) The symbols $(a, b, \ldots, g)$ and $[a, b, \ldots, g]$ denote the greatest common divisor and least common multiple, respectively, of the positive integers $a, b, \ldots, g$. For example, $(3, 6, 18) = 3$ and $[6, 15] = 30$. Prove that
$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}$.

4 Challenge Problems

1. (USAMO 2001) Let S be a set of integers (not necessarily positive) such that

   (a) there exist $a, b \in S$ with $\gcd(a, b) = \gcd(a - 2, b - 2) = 1$;

   (b) if x and y are elements of S (possibly equal), then $x^2 - y$ also belongs to S.

   Prove that S is the set of all integers.
2. If for positive integers m, n , $mn \mid m^2 + n^2 + m$ then prove that $n - 1$ is a perfect square.

JV Practice: Primes and Divisors

Ariel Uy

5 Warm-Up Problems

1. (AMC 10B '19) How many divisors of 201^9 are perfect squares? Perfect cubes? Both?
2. How many zeros are at the end of 30! ?
3. Determine if the following numbers are prime. How do you know?
   (a) 62
   (b) 71
   (c) 143
4. Suppose you're in a hallway with 100 closed lockers in a row, and 100 students walk by. The first student opens every locker. The second student closes every other locker. The third student goes to every third locker and toggles it: opens it if it's closed, and closes it if it's open. The remaining students continue this process: the n-th student goes to every n-th locker and toggles it. When all 100 students have walked by, which lockers are open?

6 Problems

1. If $528|n$ and $220|n$, find the largest a that must satisfy $a|n$.
2. Write $\gcd(a, b) \cdot \text{lcm}(a, b)$ in a different (simpler) way.
3. Find a pattern or formula to calculate the sum of the divisors of any natural number n (1 and the number itself count as divisors).

   Hint: Find the sum of all the divisors of the following numbers: $2, 3, 4, 6, 8, 9, 12, 16$. Do you notice something about prime numbers? Powers of primes?
4. (HMMT 2008) Find the smallest positive integer n such that $107n$ has the same last two digits as n.
5. (David A. Santos) Find the smallest positive integer such that $\frac{n}{2}$ is a square and $\frac{n}{3}$ is a cube.
6. (PUMaC 2011) The only prime factors of an integer n are 2 and 3. If the sum of the divisors of n (including itself) is 1815, find n.
7. Find the number of ways to write 300 as a product of three positive integers $a \cdot b \cdot c$. (The product is ordered, so $1 \cdot 3 \cdot 100$ is different from $100 \cdot 1 \cdot 3$.)
8. (ARML '14 I6) Compute the smallest number n such that $214n$ and $2014n$ have the same number of divisors.

7 Challenge Problems

1. (ARML 1978) Three positive integers are in arithmetic progression. If 1 were added to each of the two largest numbers in this progression, two primes would result. The product of the primes with the smallest of the original numbers would be 1978. Find the largest of the three original numbers.

2. (AHSME 1960) Let m and n be any two odd numbers, with n less than m. What is the largest integer which divides all possible numbers of the form $m^2 - n^2$?

3. (2008 Mock ARML) Given that the sum of all positive integers with exactly two proper divisors, each of which is less than 30, is 2397, find the sum of all positive integers with exactly three proper divisors, each of which is less than 30 (a proper divisor of n is a positive integer that divides but is not equal to n).

8 Definitions/Review

- If an integer a is divisible by an integer b, we say $b|a$, or "b divides a".

- A positive integer p is called prime if it has exactly 2 divisors: 1 and itself. An alternate, useful definition is that p is prime if when p divides a product ab (where a, b are integers), then p divides a or p divides b.

- $\gcd(a, b)$ is the greatest common divisor of two integers a and b - the largest positive integer that divides both a and b. Formally, we say $\gcd(a, b) = c$ if $c|a, c|b$, and if $d|a, d|b$ then $d|c$. The least common multiple of two integers a and b, $\text{lcm}(a, b)$, is the smallest positive integer that is a multiple of both a and b.

- The Fundamental Theorem of Arithmetic states that every nonzero integer can be written uniquely (up to order) as a product of primes.