Number theory - Modular Arithmetic

December 2019

1 Modular Arithmetic and Parity

Parity considerations can often help solve problems.

Example 1

How many functions $f : \{1, 2, \ldots, n\} \to \{2019, 2020\}$ are there such that $f(1) + f(2) + \ldots + f(2020)$ is an odd number.

Solution. We may map the numbers $1, \ldots, n-1$ to any value. Then the value of $f(n)$ determines the parity of the sum, so precisely half of the functions satisfy the property that the sum is odd. It follows that there are 2^{n-1} such functions. □

Modular arithmetic is a generalization of parity. We say $a \equiv b \pmod{n}$ if n divides $a - b$. There are n residue classes modulo n. That is every integer is congruent to one of $0, 1, 2, 3, \ldots, n-1$ modulo n. Rather than giving an account of properties of modular arithmetic, we give examples of its applications to contests.

Example 2

Let f be a nonconstant polynomial with positive integer coefficients. Show $f(n)$ divides $f(f(n)+1)$ if and only if $n = 1$.

Solution. The key observation is that

$$f(f(n) + 1) \equiv f(1) \pmod{f(n)}.$$

Now if $n = 1$, then $f(f(1) + 1) \equiv f(1) \equiv 0 \pmod{f(1)}$ and $f(n)$ divides $f(f(n) + 1)$.
Conversely, suppose $n > 1$. Since f has positive integer coefficients, it is an increasing function on positive numbers, hence $f(n) > f(1)$ whenever $n > 1$. It follows that $f(f(n) + 1) \equiv f(1) \not\equiv 0 \pmod{f(n)}$ so $f(n)$ does not divide $f(f(n) + 1)$. □

1.1 Problems

1. Show that among any three distinct integers, we can find two, say a and b, such that $ab^3 - a^3b$ is divisible by 10.

2. Let
$$p(x) = a_n x^n + \ldots + a_1 x + a_0$$
be a polynomial with integer coefficents such that $p(0)$ and $p(1)$ are odd numbers. Show p has no integer roots.

3. Find all integers $n > 1$ such that any prime divisor of $n^6 - 1$ is also a divisor of $(n^3 - 1)(n^2 - 1)$.

4. Let p be an odd prime number. For each $i = 1, 2, 3, \ldots, p-1$, let r_i denote the remainder of i^p divided by p^2. Compute the sum
$$r_1 + r_2 + \ldots + r_{p-1}.$$

2 Fermat's Little Theorem

Theorem 1: Fermat's Little Theorem

Let p be a prime number. Then
$$a^p \equiv a \pmod{p}.$$

Example 3

Let p be an odd prime. Show there are infinitely many positive integers n for which p divides $2^n - n$.

Solution. We claim that if $n = (p-1)^{2k}$, then p divides $2^n - n$, where $k \geq 1$ is an integer. Indeed, $n \equiv (-1)^{2k} \equiv 1 \pmod{p}$, so it suffices to show $2^n \equiv 1 \pmod{p}$. Fermat's little theorem gives $2^{p-1} \equiv 1 \pmod{p}$ hence
$$2^n \equiv (2^{p-1})^{(p-1)^{2k-1}} \equiv 1^{(p-1)^{2k-1}} \equiv 1 \pmod{p},$$
and we are done. □

2.1 Problems

5. Let $k = 2008^2 + 2^{2008}$. What is the unit digit of $2^k + k^2$?

6. Find n such that $n^5 = 27^5 + 84^5 + 110^5 + 133^5$.

7. Let p be a prime not equal to 2, 3 or 5. Let n be the $p-1$ digit number all of whose digits are 1. Show that n is divisible by p.

8. Let $p > 2$ be a prime number and n a positve integer. Prove that p divides $1^{p^n} + 2^{p^n} + \ldots + (p-1)^{p^n}$.

9. Let p be an odd prime. If the equation $x^2 \equiv a \pmod{p}$ has a solution, then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Use this to conclude that there are infinitely many primes of the form $4k + 1$.

10. Prove that the sequence $2^n - 3$ contains an infinite subsequence whose terms are pairwise relatively prime.

3 Euler's Theorem

Theorem 2: Euler's (Totient) Theorem

If a and n are relatively prime, then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ denotes the number of positive integers up to n which are relatively prime to n.

The next example will require the *Chinese Remainder Theorem*. The statement is a bit technical but the idea very simple so we will not state the result but rather give a brief example describing the main idea. Say we have x bottles of beer and if we divide it by $n = 14$ there are 8 bottles leftover, and if we divide it by $m = 3$ there's one bottle leftover. The Chinese remainder theorem says that provided n and m are relatively prime, x has a unique residue class modulo the product nm. That is if we divide our number of beer bottles by $42 = 3 \times 14$, then there *must* be 22 bottles leftover (it's easy to check $22 \equiv 8 \pmod{14}$ and $22 \equiv 1 \pmod{3}$).

Example 4

Find the last 3 *digits on* $2003^{2002^{2001}}$.

Solution. We claim the last three digits are 241.
It suffices to compute the residue of $2003^{2002^{2001}} \pmod{1000}$. We have

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}.$$

Euler's theorem says we may take the exponent 2002^{2001} modulo $\varphi(1000)$. Note that $\varphi(1000) = 400$. We have

$$2002^{2001} \equiv 2^{2001} \pmod{400}.$$

We have $2^{2001} \equiv 0 \pmod{16}$ and by Euler's theorem, we find $2^{2001} \equiv (2^{20})^{100} \times 2 \equiv 2 \pmod{25}$ (since $\varphi(25) = 20$). By the Chinese Remainder theorem, we conclude

$$2^{2001} \equiv 352 \pmod{400}.$$

Euler's theorem then gives that

$$3^{2002^{2001}} \equiv 3^{352} \pmod{1000}.$$

This can either be bashed out, or computed cleverly using the binomial theorem. We have $3^{352} = 9^{176} = (10-1)^{176}$, so looking mod 1000,

$$3^{352} \equiv \binom{176}{2}10^2 - \binom{176}{1}10 + 1 \equiv 241 \pmod{1000},$$

proving the claim. □

3.1 Problems

11. Find the units digit of $7^{7^{7^{\cdot^{\cdot^{\cdot^{7}}}}}}$, where there are 1001 7's

12. Show there exists two different powers of 3 whose difference is divisible by 2020.

13. Show that if p and q are distinct primes, then for every integer a, the number pq is a divisor of $a^{pq-p-q+2} - a$.

14. Show that for any positive integer s, there is a positve integer n whose sum of digits is s and for which $s|n$.

15. Let $a > 1$ be an odd positive integer. What is the smallest integer n such that 2^{2000} is a divisor of $a^n - 1$. (Note your answer may depend on a).

4 Wilson's Theorem

Theorem 3: Wilson's Theorem

A positive integer n is prime if and only if

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

4.1 Problems

16. Suppose a and n are relatively prime positive integers with $n \geq 2$. Prove that

$$a^{n-1} + (n-1)! \equiv 0 \pmod{n}$$

if and only if n is prime.

17. For each positive integer n, find the greatest common divisor of $n! + 1$ and $(n+1)!$.

18. Let $p \geq 3$ be a prime number, and suppose

$$\{a_1, a_2, \ldots, a_p\} \quad \{b_1, b_2, \ldots, b_p\}$$

are two sets of complete residue classes modulo p. Prove that

$$a_1 b_1, a_2 b_2, \ldots, a_p b_p$$

is not a complete set of residue classes modulo p.