Modular Arithmetic

Epsilon Summer Series

July 16, 2015

1 Basics of Modular Arithmetic

For a positive integer n, and integers a and b, we define

$$a \equiv b \pmod{n}$$

if a and b have the same remainder upon division by n (so n divides $a - b$).

We can do arithmetic "working mod n" the same way we do normal arithmetic - addition, subtraction, multiplication, and exponentiation all work the same. For example:

$$9 * 7 \equiv 4 * 2 \equiv 8 \equiv 3 \pmod{5}$$

and

$$3^{12} \equiv 27^4 \equiv (-1)^4 \equiv 1 \pmod{7}$$

Remember, we can use negative numbers too!
Unfortunately, division doesn't work (see why?). This is why it is convenient to use prime numbers. Often in modular congruence problems instead of simply looking mod$n$, we want to look mod$p$, where p is a prime dividing n.

2 Prime factorizations

We can write any number as the product of its prime divisors, so

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

The number of divisors of n is

$$(e_1 + 1)(e_2 + 1) \dots (e_k)$$

The sum of the divisors of n is

$$(1 + p_1 + p_1^2 \dots p_1^{e_1})(1 + p_2 + p_2^2 \dots p_2^{e_2}) \dots (1 + p_k + p_k^2 \dots p_k^{e_k})$$

Finally, the number of positive integers less than n and relatively prime to n is defined as

$$\phi(n) = (p_1^{e_1} - p_1^{e_1 - 1})(p_2^{e_2} - p_2^{e_2 - 1}) \dots (p_k^{e_k} - p_k^{e_k - 1}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k})$$

$\phi(n)$ is known as Euler's totient function or the "phi" function

3 More advanced stuff

For this section let p be a prime.

If a is not 0 mod p, then it has a unique inverse x (so $ax \equiv 1 \pmod{p}$).This allows us to "divide" by any non-zero residue, by simply multiplying by the inverse
ex) Find the inverse of 3 (mod 7)
ex) Solve the equation $3x \equiv 2 \pmod{7}$

3.1 Theorems!

Fermat's Little Theorem: If $gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Wilson's Theorem:

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

Euler's Totient Theorem: Let $\phi(n)$ be the phi function. Then if $gcd(a, n) = 1$,

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

Chinese Remainder Theorem: If, $\gcd(m, n) = 1$, then there exists exactly 1 solution, mod mn, to the system

$$x \equiv r \pmod{m}$$
$$x \equiv s \pmod{n}$$

4 Problems

1. Determine the remainder when $12351 + 12451252 + 1626216126$ is divided by 4.
2. Determine the remainder when $12351 * 12451252 * 1626216126$ is divided by 5.
3. Determine the last two digits of 7^{1942}
4. Adam and Ben start their new jobs on the same day. Adam's schedule is 3 workdays followed by 1 rest day. Ben's schedule is 7 workdays followed by 3 rest days. On how many of their first 1000 days do both have rest-days on the same day?
5. Determine the number of divisors and sum of divisors of the number 420.
6. Let x and y be positive integers such that $7x^5 = 11y^{13}$. What is the minimum possible value of x? (Just the prime factorization is fine)
7. What is the largetst integer which must evenly divide all integers of the form $n^5 - n$
8. Prove that if p and $p + 2$ are both prime integers greater than 3, then 6 is a factor of $p + 1$
9. Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

   (a) If 16, 15, or 14 students are present, then in each case all the blocks can be distributed in equal numbers to each student, and
   (b) There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

   Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.
10. For a positive integer p, define the positive integer n to be p-safe if n differs in absolute value by more than 2 from all multiples of p. For example, the set of 10-safe numbers is $3, 4, 5, 6, 7, 13, 14, 15, 16, 17, 23, ...$ Find the number of positive integers less than or equal to $10,000$ which are simultaneously 7-safe, 11-safe, and 13-safe.
11. Find all positive integers n for which $2^n + 12^n + 2011^n$ is a perfect square.

5 Answers

1. 1
2. 2
3. 49
4. 100
5. number: 24; sum: 1344
6. 7^5 11^8
7. 30
8. Skeleton for proof: p and $p+2$ must both be 1 (mod 2), while p and $p+2$ must also be 2 (mod 3) and 1 (mod 3), respectively.
9. 148
10. 958
11. 1 is the only solution. Show using mod 3 and mod 4.