Remainders and Modular Arithmetic

Lemma 1. Let *a, d* be integers, *d*>0. Then there exist unique integers *q* and *r,* such that $a = qd + r$ and $0 \le r < b$.

Definition. The number *q* is called the *quotient*, while *r* is called the *remainder modulo d*.

2. The difference of two integers is divisible by *d* **iff** these integers have the same remainder modulo *d*.

Definition. This can be written short as $m \equiv n \pmod d$ or just $m \equiv_d n$.

3. Prove that the remainder of any prime module 30 is either a prime or 1.

Theorem 4 *(modular arithmetic)*. Let the integer a_1 has the remainder r_1 mod *d* , and the integer a_2 has the remainder r_2 mod *d* . Then integers a_1+a_2 , a_1-a_2 , a_1a_2 has the same remainders modulo *d* as integers r_1+r_2, r_1-r_2, r_1r_2.respectively.

5. Find the last digit in the decimal expression of $777^{555^{333}}$.

6. Let *x* and *y* be positive integers. Prove that

a) $x^3 \equiv_{10} y^3 \Leftrightarrow x \equiv_{10} y$

b) If $10 \mid (x^2+xy+y^2)$ then $100 \mid (x^2+xy+y^2)$

7. The sum of a few odd perfect squares is 2015. Find the minimum number of terms in the sum.

If the polynomial equation has an integer solution, it has a solution modulo any positive integer. And vice versa: if the equation has no solution module some positive integer it has no integer solution.

9. Prove that

a) the equation $n^2+1=0$ (mod 3) has no solution.

b) he equation $n^2+1=3m$ has no integer solution.

10. Prove that the following equations has no integer solutions :

a) $x^2+y^2=4z-1$ **b)** $15x^2-7y^2=9$ **c)** $x^2+y^2+z^2=8t-1$

Theorem 11 *(remainder cancellation)*.

Let *m* and *b* be coprime. Then $ma_1 \equiv_b ma_2 \Leftrightarrow a_1 \equiv_b a_2$.

12. Let *m* is not divisible by the prime *p*. Prove that

a) Remainders of the integers *m*, 2*m*, 3*m*, …, (*p*–1)*m* modulo *p* are distinct.

b) Remainders of (*p*–1)! and m^{p-1}(*p*–1)! modulo *p* are the same.

c) *(Fermat's little theorem)*. $p \mid m^{p-1}-1$

13. Let *n* be a positive integer not divisible by 17. Show that either $17 \mid n^8+1$, or $17 \mid n^8-1$.

14. Find the remainder of 50^{10000} (mod 101)

15. Prove that for every prime *p*>5 the integer 11...1 ($p-1$ digits) is divisible by p.

16. a) Let *m* be an integer not divisible by the prime *p*. Prove that there is exactly one $n \in \{1, 2, \ldots, p-1\}$ such that $mn \equiv_p 1$.

b) Prove that for every prime *p*>2 there are exactly two integers among 1, 2, …, *p*–1 which squares are 1 modulo *p*.

c) (*Wilson's theorem***)** Prove that $p \mid (p-1)!+1$ iff *p* is prime or *p*=1.

Extra problems

Re1. Given 100 integers such that the sum of any 99 of them is divisible by 13. Prove that each of the integers is divisible by 13.

Re2. An integer *N* is given to Mateo. He divides *N* by 101 and gets the remainder *m*>0. Then Mateo divides *N* by *m* and gets the remainder *p*. Find the maximum possible value for *p* and the least possible value for *N* to get this value for *p*.

Re3* Prove that

a) If a prime $p \equiv_4 3$, then the equation $x^2 = -1$ has no solution modulo *p.*

b) If $p \mid n^2+1$ for an integer *n*, then $p \equiv_4 1$

c) there are infinitely many primes $p \equiv_4 1$

Re4. Prove that for every positive integer *n* there exist two consecutive positive integers less then 10^n such that their product is divisible by 10^n .

IMC2007.1.1 Let *f* be a polynomial of degree 2 with integer coefficients. Suppose that *f*(*k*) is divisible by 5

for every integer k. prove that all coefficients of f are divisible by 5.

IMC2007.2.2 Let x, y, z be integers such that $S = x^4 + y^4 + z^4$ is divisible by 29. Show that S is divisible by 29^4

www.ashap.info/Uroki/eng/NYUAD15/index.html