Lecture 11: Some divisibility tests

A very special application of congruence theory involves finding special criteria under which a given integer is divisible by another integer.

Theorem 11.1 For any integer $b>1$ any positive integer N can be written uniquely in terms of powers of b as:

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients can take on the b different values $0, 1, 2, \ldots, b-1$.

Proof Applying Division algorithm on N and b: we get integers q_1 and a_0 such that $N = q_1 b + a_0 \quad 0 \leq a_0 < b$

If $q_1 \geq b$ then we divide again to get:

$$q_1 = q_2 b + a_1 \qquad 0 \leq a_1 < b$$

Hence
$$N = (q_2 b + a_1) b + a_0 = q_2 b^2 + a_1 b + a_0$$

If $q_2 \geq b$ then proceeding similarly as above gives us:

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Since $N > q_1 > q_2 > \cdots \geq 0$ is a strictly decreasing sequence of integers, this process must eventually terminate say at $(m-1)^{th}$ stage giving us:

$$N = q_m b^m + q_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

Putting $a_m = q_m$ we have:

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

Next we show that this representation is unique.

Suppose N has two distinct representations:

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0 = c_m b^m + c_{m-1} b^{m-1} + \cdots + c_1 b + c_0$$

where $0 \leq a_i < b \;\; \forall\, i$ and $0 \leq c_j < b \;\; \forall\, j$ (we can use the same m by simply adding terms with coefficients $a_i = 0$ OR $c_j = 0$ if necessary)

Subtracting the second representation from the first gives us:

$$N - N = (a_m - \cancel{b}\, c_m) b^m + \cdots + (a_1 - c_1) b + (a_0 - c_0)$$

i.e. $0 = d_m b^m + \cdots + d_1 b + d_0$ where $d_i = 0$ for $i = 0, 1, \ldots, m$

By assumption $d_i \neq 0$ for some i. Let k be the smallest subscript for which $d_k \neq 0$. Then

$$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$$

$$\Rightarrow 0 = d_m b^{m-k} + \cdots + d_{k+1} b + d_k$$

$$\Rightarrow d_k = -\left(d_m b^{m-k} + \cdots + d_{k+1} b\right)$$

$$\Rightarrow d_k = -b\left(d_m b^{m-k-1} + \cdots + d_{k+1}\right)$$

$$\Rightarrow b \mid d_k$$

From the inequalities $0 \leq a_k < b$ and $0 \leq c_k < b$ ($\Rightarrow -b < -c_k < 0$)

We have: $0 - b < a_k - c_k < b + 0$ i.e. $-b < d_k < b$ i.e. $|d_k| < b$

This is possible only when $d_k = 0$

This is a contradiction. Hence N must be unique.

* <u>Note</u> We can also write N as:

$N = (a_m a_{m-1} \cdots a_1 a_0)_b \leftarrow$ base b place-value notation for N

Example: Calculate $5^{110} \pmod{131}$.

Solution: We will use a method so-called the "binary exponential algorithm"

$$110 = 64+32+8+4+2$$

$$= 1\cdot 2^6 + 1\cdot 2^5 + 0\cdot 2^4 + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0\cdot 2^0$$

$$= (110110)_2$$

We obtain ~~po~~ the powers 5^{2^j}, $0 \leq j \leq 6$

$$5^2 \equiv 25 \pmod{131}$$

$$5^4 \equiv 625 \pmod{131} \equiv 101 \pmod{131}$$

$$5^8 \equiv 114 \pmod{131}$$

$$5^{16} \equiv 27 \pmod{131}$$

$$5^{32} \equiv 74 \pmod{131}$$

$$5^{64} \equiv 105 \pmod{131}$$

Hence $5^{110} = 5^{64+32+8+4+2}$

$$= 5^{64}\cdot 5^{32}\cdot 5^8\cdot 5^4\cdot 5^2$$

$$= 105\cdot 74\cdot 114\cdot 101\cdot 25 \equiv 60 \pmod{131}$$

Thm 11.2 Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{m}$ then $P(a) \equiv P(b) \pmod{m}$

Proof Since $a \equiv b \pmod{m}$

Therefore $a^k \equiv b^k \pmod{m}$ $\quad \forall\, k = 0, 1, \ldots, m$

$$\Rightarrow c_k a^k \equiv c_k b^k \pmod{m}$$

Adding all such congruences we have:

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{m}$$

i.e. $P(a) \equiv P(b) \pmod{m}$

Corollary 11.3 If a is a solution of $P(x) \equiv 0 \pmod{m}$ and $a \equiv b \pmod{m}$ then b is also a solution of $P(x) \equiv 0 \pmod{m}$.

Proof. [a is a solution of $P(x) \equiv 0 \pmod{m}$ if $P(a) \equiv 0 \pmod{m}$]

Since $a \equiv b \pmod{m}$ hence

$$P(a) \equiv P(b) \pmod{m}$$

Also since a is a solution of $P(x) \equiv 0 \pmod{m}$, therefore

$$P(a) \equiv 0 \pmod{m}$$

$$\Rightarrow P(b) \equiv 0 \pmod{m}$$

Therefore b is also a solution of $P(x) \equiv 0 \pmod{m}$

Divisibility test for 9

Thm 11.4 Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$ and let $S = a_0 + a_1 + \cdots + a_m$. Then $9 \mid N$ if and only if $9 \mid S$.

Proof Let us consider the polynomial $P(x) = \sum_{k=0}^{m} a_k x^k$

Since $10 \equiv 1 \pmod{9}$, hence

$$P(10) \equiv P(1) \pmod{9}$$

$$\Rightarrow N \equiv S \pmod{9}$$

Note that $N \equiv 0 \pmod{9}$ if and only if $S \equiv 0 \pmod{9}$

Hence $9 \mid N$ if and only if $9 \mid S$.

Divisibility test for 11

Thm 11.5 Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$ and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid T$.

Proof Let us consider the polynomial $P(x) = \sum_{k=0}^{m} a_k x^k$

Since $10 \equiv -1 \pmod{11}$

Hence $P(10) \equiv P(-1) \pmod{11}$

$$\Rightarrow N \equiv T \pmod{11}$$

Since $N \equiv 0 \pmod{11}$ if and only if $T \equiv 0 \pmod{11}$

Therefore $11 \mid N$ if and only if $11 \mid T$.

Exercise:

1) Use the binary exponentiation algorithm to compute $19^{53} \pmod{503}$ and $141^{47} \pmod{1537}$

2) Prove the following:

(a) For any $a \in \mathbb{Z}$ the unit digit of a^2 is 0, 1, 4, 5, 6 or 9.

(b) ,, ,, ,, ,, ,, ,, ,, a^4 is 0, 1, 5 or 6.

3) Find the last two digits of the number 9^{9^9}.

4) Establish the following:

(a) An integer is divisible by 2 $\Longleftrightarrow$ its unit digits are even.

(b) ,, ,, ,, ,, ,, 3 $\Longleftrightarrow$ the sum of its digits is divisible by 3

(c) ,, ,, ,, ,, ,, 5 $\Longleftrightarrow$ its unit digit is 0 or 5.

(d) ,, ,, ,, ,, ,, 4 $\Longleftrightarrow$ the number formed by its tens and unit digit is divisible by 4.