Congruence

Putnam practice

November 12, 2003

We say a is *congruent* to b *modulo* n and write $a \equiv b(\text{mod } n)$ if $n|(a-b)$. Let p be a prime and $\mathbb{Z}_p$ denote the set $\{0, 1, ...p-1\}$. Define $+$ and $\cdot$ on $\mathbb{Z}_p$ using congruence modulo p. The system $(\mathbb{Z}_p, +, \cdot)$ is a finite field.

Example 1 *Prove that* $36^{36} + 41^{41}$ *is divisible by* 77.

Solution: Note $41 \equiv -36(\text{mod } 77)$. Thus

$$36^{36} + 41^{41} \equiv 36^{36} + (-36)^{41} \equiv 36^{36}(1 - 36^5)(\text{mod } 77)$$

Also note

$$36 \equiv 1(\text{mod } 7)$$

and

$$36^5 \equiv 3^5 \equiv 1(\text{mod } 11)$$

Thus

$$36^5 \equiv 1(\text{mod } 77)$$

and we are done.

Theorem 1 (Fermat's Little Theorem) *If p is prime and a is not divisible by p, then*

$$a^{p-1} \equiv 1(mod\ p)$$

Euler's function is given by $\phi(m) = m \prod_{p|m}(1 - 1/p)$.

Theorem 2 (Euler's Theorem) *If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1(mod\ m)$.*

Example 2 *Find the last three digits of 7^{9999}.*

Solution: Since $\phi(1000) = 1000(1/2)(4/5) = 400$, we know from Euler's Theorem that

$$7^{1000} = (7^{400})^{25} \equiv 1(\text{mod } 1000)$$

Note that $7 \cdot 143 = 1001 \equiv 1(\text{mod } 1000)$. Then

$$7^{9999} \equiv 143 \cdot 7 \cdot 7^{9999} = 143 \cdot 7^{10000} \equiv 143(\text{mod } 1000)$$

Example 3 *Prove that there is no integer $n > 1$ for which $n|(2^n - 1)$.*

Solution: We use the Well-Ordering Principle. Suppose that the set

$$S = \{n|n > 1, n|(2^n - 1)\}$$

is non-empty and let m be its smallest element. Clearly m must be odd. Then by Euler's Theorem $m|(2^{\phi(m)} - 1)$. Let $m = \phi(m)q + r, 0 \leq r < \phi(m)$, then

$$2^m - 1 = (2^{\phi(m)} - 1)(2^{m-\phi(m)} + ... + 2^{m-q\phi(m)}) + 2^r - 1$$

Thus

$$(2^m - 1, 2^{\phi(m)} - 1) = (2^{\phi(m)} - 1, 2^r - 1)$$

Let $d = (m, \phi(m))$. By applying the equation above possibly several times we get

$$(2^m - 1, 2^{\phi(m)} - 1) = 2^d - 1$$

Then $m|2^d - 1$. Note that then $d > 1$. Also $d|(2^d - 1)$ because $d|m$ and $m|(2^d - 1)$. Since $d \leq \phi(m) \leq m$ we reached a contradiction by producing an element $d \in S$ that is smaller than m.

Theorem 3 *Let P be a polynomial with integral coefficients, and let a and b be arbitrary integers. Then $P(a) - P(b)$ is divisible by $a - b$.*

Theorem 4 *Let $s(n)$ denote the sum of the digits in the decimal representation of n. Then $n \equiv s(n)(mod\ 9)$.*

Theorem 5 (Chinese Remainder Theorem) *Suppose that $m_1, m_2, ...m_k$ are pairwise relatively prime and $a_1, a_2, ...a_k$ are arbitrary integers. Then there exist solutions of the simultaneous congruences*

$$x \equiv a_i(mod\ m_i)$$

Any two solutions are congruent modulo $M = m_1 m_2 ... m_k$.

1 Problems

1. Prove that $19^{19} + 69^{69}$ is divisible by 44.

2. Find the last 3 digits of 13^{398}.

3. What powers of 2 give a remainder of 15 when divided by 17?

4. Denote by $S(m)$ the sum of the digits of the positive integer m. Prove that there does not exist a number N such that $S(n) \leq S(n+1)$ for all $n \geq N$.

5. Find the fifth digit from the end of the number $5^{5^{5^{5^5}}}$.