

Notes 3/25/08

Congruences - Part II

Proposition 1. *Let p be prime and $a, b \in \mathbb{Z}$. Then*

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

Proof. By the binomial theorem,

$$(a + b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{p-1}ab^{p-1} + b^p$$

We have proved that a prime p divides $\binom{p}{1}, \binom{p}{2}, \dots, \binom{p}{p-1}$ and hence all the middle terms in the binomial formula are equal to zero modulo p and we get

$$(a + b)^p \equiv a^p + b^p \pmod{p}$$

□

Theorem 2. (*Fermat's Little Theorem*) *If p is prime then then for every $a \in \mathbb{Z}$*

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

Proof. We first consider the case when $a > 0$ and proceed by induction on $a \geq 0$. The base case, $a = 0$, is trivial. For the inductive step, we assume that

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

and we want to deduce

$$(a + 1)^p \equiv a + 1 \pmod{p}.$$

Using both the above proposition and inductive assumption we have

$$(a + 1)^p \equiv a^p + 1 \pmod{p} \equiv a + 1 \pmod{p}.$$

Now, for a negative a we already know that

$$(-a)^p \equiv -a \pmod{p}$$

since $-a$ is positive and we have proved the theorem for positive a . If prime $p \neq 2$, then p is odd and the above rewrites

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

Multiplying this by -1 we get the desired formula. It remains to consider the case $p = 2$. That is, we want to show

$$a^2 \equiv a \pmod{2},$$

2

or $2 \mid a^2 - a = a(a - 1)$ which is plainly true as one of the two consecutive integers $a, a - 1$ is even. \square

Corollary 3. *If p is prime then for every $a \in \mathbb{Z}$ such that $p \nmid a$*

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

Example 1. Find the remainder after dividing 2^{100} by 101.

We apply the corollary with $a = 2, p = 101$ and see that the remainder is 1.

How to Solve Congruences

We start with the simplest case. Given $b \in \mathbb{Z}$ and $m \in \mathbb{N}$ we want to find x such that

$$x \equiv b \pmod{m}.$$

this is equivalent to $m \mid x - b$, that is, $x - b = mk$ for an integer k and we get

$$x = b + mk, \quad k \in \mathbb{Z}$$

which describes all the solutions to the congruence.

Example 2. Solve for x

$$x \equiv 7 \pmod{11}.$$

Clearly, $x = 7$ would work and so would $x = 18, 29, 40, \dots$ and $x = -4, -15, -26, \dots$. We can write all these solutions as

$$x = 7 + 11k, \quad k \in \mathbb{Z}$$

Next, we consider a congruence with a coefficient in front of x

$$ax \equiv b \pmod{m}$$

where we require that $\gcd(a, m) = 1$. The case when the gcd is not 1 is on the homework.

Example 3. Solve for x

$$3x \equiv 5 \pmod{13}.$$

We would like to get rid of the coefficient 3 in front of x here. If we multiply 3 by 9 we get 27, which is 1 modulo 13 and this takes care of the coefficient in front of x :

$$27x \equiv 45 \pmod{13}$$

$$26x + x \equiv 6 \pmod{13}$$

$$x \equiv 6 \pmod{13}$$

and

$$x = 6 + 13k, \quad k \in \mathbb{Z}.$$

Let's show that we can always get rid of the coefficient in front of x in

$$ax \equiv b \pmod{m}.$$

Since $\gcd(a, m)=1$, there exist integers s and t such that

$$as + tm = 1$$

Let's multiply the congruence by s

$$asx \equiv bs \pmod{m}.$$

Since $as = 1 - tm$, we get

$$x - tmx \equiv bs \pmod{m}.$$

Now reducing modulo m we get

$$x \equiv bs \pmod{m},$$

and the solutions are

$$x = bs + mk, \quad k \in \mathbb{Z}$$

We have proved

Theorem 4. *Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, and $\gcd(a, m) = 1$. Then the congruence*

$$ax \equiv b \pmod{m}$$

always has a solution and all the solutions are congruent modulo m .

Now we consider a system of congruences

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv b' \pmod{m'} \end{cases}$$

where $\gcd(m, m') = 1$

As with systems of linear equations, we solve the first congruence, get

$$x = b + mk, \quad k \in \mathbb{Z}$$

and plug in the result into the second

$$mk + b \equiv b' \pmod{m'}$$

$$mk \equiv b' - b \pmod{m'}$$

Here the variable is k , $\gcd(m, m')=1$ and we can apply Theorem 4 to solve the congruence. Since $\gcd(m, m')=1$, we can find integers s and s' such that

$$ms + m's' = 1,$$

multiply the congruence by s

$$msk \equiv s(b' - b) \pmod{m'},$$

4

plug in $1 - m's'$ for ms

$$k - km's' \equiv s(b' - b) \pmod{m'}$$

reduce the result modulo m

$$k \equiv s(b' - b) \pmod{m'}$$

get

$$k = s(b' - b) + lm' \quad l \in \mathbb{Z}$$

and plug this into $x = b + mk$

$$x = b + mk = b + m(s(b' - b) + lm') = m + (b' - b)sm + lm'm \quad l \in \mathbb{Z}.$$

We have proved

Theorem 5. (*Chinese Remainder Theorem*) Let $b, b' \in \mathbb{Z}$, $m \in \mathbb{N}$. Let $\gcd(m, m') = 1$ then the system of congruences

$$\begin{cases} x \equiv b \pmod{m} \\ x \equiv b' \pmod{m'} \end{cases}$$

has a solution and all its solutions are congruent modulo mm' .

Example 4. Solve for x

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{13} \end{cases}$$

From the first congruence, $x = 2 + 5k$, where $k \in \mathbb{Z}$. Plug this into the second congruence, get

$$2 + 5k \equiv 5 \pmod{13}$$

$$5k \equiv 3 \pmod{13}$$

If we multiply the congruence 8 we will get rid of the coefficient

$$40k \equiv 24 \pmod{13}$$

$$k \equiv 11 \pmod{13}$$

We get $k = 11 + 13l$ where $l \in \mathbb{Z}$. Hence

$$x = 2 + 5k = 2 + 5(11 + 13l) = 57 + 65l, \quad l \in \mathbb{Z}.$$