PITHAPUR RAJAH'S GOVERNMENT (A)COLLEGE: KAKINADA
DEPARTMENT OF MATHEMATICS

SEMESTER -V: NUMBER THEORY

CONGRUENCES

BY

KARNIKOTI. SAMRAJYAM M.Sc ,B.E.d, M.Phill

Lecturer in Mathematics

Congruences and Congruence Equations

A great many problems in number theory rely only on *remainders* when dividing by an integer. Recall the division algorithm: given $a \in \mathsf{Z}$ and $n \in \mathsf{N}$ there exist unique $q, r \in \mathsf{Z}$ such that

$$a = qn + r, \qquad 0 \leq r < n \qquad (*)$$

It is to the *remainder* r that we now turn our attention.

3.1 Congruences and Z_n

Definition 3.1. For each $n \in \mathsf{N}$, the set $\mathsf{Z}_n = \{0, 1, \ldots, n-1\}$ comprises the *residues modulo n.* Integers a, b are said to be *congruent modulo n* if they have the same residue: we write $a \equiv b \pmod{n}$.

The division algorithm says that every integer $a \in \mathsf{Z}$ has a unique *residue* $r \in \mathsf{Z}_n$.

Example 3.2. We may write $7 \equiv -3 \pmod{5}$, since applying the division algorithm yields

$$7 = 5 \times 1 + 2 \text{ and } \quad -3 = 5 \times (-1) + 2$$

Indeed both 7 and 12 have residue 2 modulo 5.

As another example, we prove a very simple result.

Lemma 3.3. *All squares of integers have remainders 0 or 1 upon dividing by 3.*

Theorem 3.4. $a \equiv b \pmod{n} \iff n \mid (a-b)$

Proof. Suppose that $a = q_1 n + r_1$ and $b = q_2 n + r_2$ are the results of applying the division algorithm to a, b modulo n. Plainly $a \equiv b \pmod{n} \iff r_1 = r_2$. We prove each direction separately:

($\Rightarrow$) This is almost immediate:

$$r_1 = r_2 \implies a - nq_1 = b - nq_2 \implies a - b = n(q_2 - q_1)$$

Since $q_2 - q_1$ is an integer, $a - b$ is a multiple of n.

($\Leftarrow$) Conversely, suppose that $a - b = kn$ is a multiple of n. Then

$$r_1 - r_2 = (a - nq_1) - (b - nq_2) = (a - b) + n(q_2 - q_1) = n(k + q_2 - q_2)$$

This says that $r_1 - r_2$ is an integer multiple of n. Recalling the proof of the division algorithm, $-n < r_1 - r_2 < n$ forces $r_1 - r_2 = 0$. ∎

The Theorem says that we can compare remainders *without computing quotients.* In case the advantage isn't clear, we recall our earlier example.

Example (3.2 revisited). $7 \equiv -3 \pmod{5}$ follows since $7 - (-3) = 10$ is divisible by 5. There is no need for us to express 7 and -3 using the division algorithm.

Our next goal is to define an *arithmetic* with remainders, again *without* calculating quotients.

Example 3.5. If $x \equiv 3$ and $y \equiv 5 \pmod{7}$, then there exist integers k, l such that $x = 7k + 3$ and $y = 7l + 5$. But then

$$xy = 7(7kl + 5k + 3l) + 15 = 7(7kl + 5k + 3l + 2) + 1 \implies xy \equiv 1 \pmod{7}$$

It would be so much simpler if we could write

$$x \equiv 3,\ y \equiv 5 \implies xy \equiv 3 \cdot 5 \equiv 15 \equiv 1 \pmod{7}$$

Thankfully the next result justifies the crucial step.

Theorem 3.6 (Modular Arithmetic). *Suppose that $x \equiv a$ and $y \equiv b \pmod{n}$. Then*

1. $x \pm y \equiv a \pm b \pmod{n}$
2. $xy \equiv ab \pmod{n}$
3. *For any $m \in \mathbb{N}$, $x^m \equiv a^m \pmod{n}$*

Proof. We just prove 2: part 1 is similar, and part 3 is by induction using part 2 as the induction step. By Theorem 3.4, there exist integers k, l such that $x = kn + a$ and $y = ln + b$. But then

$$xy = (kn + a)(ln + b) = n(kln + al + bk) + ab \implies xy \equiv ab \pmod{n}$$

∎

Examples 3.7. We can now easily compute remainders of complex arithmetic objects.

1. What is the remainder when 17^{113} is divided by 3?

   Don't bother asking your calculator: 17^{113} is 139 digits long! Instead we use modular arithmetic:

   $$17 \equiv -1 \pmod 3 \implies 17^{113} \equiv (-1)^{113} \qquad \text{(Theorem 3.6, part 3.)}$$
   $$\equiv -1 \pmod 3 \qquad \text{(since 113 is odd)}$$

   Since $-1 \equiv 2$, we conclude that 17^{113} has remainder 2 when divided by 3.

2. Similarly, calculating remainders modulo 10 yields

   $$219^{45} - 43^{12} \equiv (-1)^{45} - 3^{12} \equiv -1 - 9^6 \equiv -1 - (-1)^6 \equiv -1 - 1 \equiv -2 \equiv 8 \pmod{10}$$

3. We find the remainder when 4^{49} is divided by 67. Even with the assistance of a powerful calculator, evaluating

   $$4^{49} = 316,912,650,057,057,350,374,175,801,344$$

   doesn't help us! Instead we first search for a power of 4 which is *small* modulo 67: the obvious choice is $4^3 = 64$.

   $$4^{49} \equiv 4 \cdot (4^3)^{16} \equiv 4 \cdot (-3)^{16} \equiv 4 \cdot 3^{16} \pmod{67}$$

   Next we search for a power of 3 which is small: since $3^4 = 81 \equiv 14 \pmod{67}$ we obtain

   $$4^{49} \equiv 4 \cdot (3^4)^4 \equiv 4 \cdot 14^4 \pmod{67}$$

   Now observe that $14^2 = 196 \equiv -5 \pmod{67}$ and we are almost finished:

   $$4^{49} \equiv 4 \cdot (-5)^2 \equiv 4 \cdot 25 \equiv 100 \equiv 33 \pmod{67}$$

Now that we have some better notation, here is a much faster proof of Lemma 3.3.

Proof. Modulo 3 we have:

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 4 \equiv 1$$

Hence squares can only have remainders 0 or 1 modulo 3. ∎

As an application, we can easily show that in a primitive Pythagorean triple (a, b, c) exactly one of a or b is a multiple of three. Just think about the remainders modulo 3:

$$a^2 + b^2 \equiv c^2 \pmod 3$$

The only possibilities are $0 + 0 \equiv 0$, $0 + 1 \equiv 1$ and $1 + 0 \equiv 1$, however the first says that all three of a, b, c are divisible by three which results in a non-primitive triple.

Similar games can be played with other primes.

Congruence and Division By Theorem 3.6, we may add, subtract, multiply and take positive integer powers of remainders without issue. Division is another matter entirely: it simply does not work in the usual sense.

Example 3.8. Since $54 - 30 = 24$ is divisible by 8, we see that $54 \equiv 30 \pmod 8$. We'd like to divide both sides this congruence by 6, however

$$6 \times 9 \equiv 6 \times 5 \pmod 8 \not\Longrightarrow 9 \equiv 5 \pmod 8$$

since the right hand side is *false.* What can we try instead? Instead we follow the definition:

$$6 \times 9 \equiv 6 \times 5 \pmod 8 \Longrightarrow 6 \times 9 = 6 \times 5 + 8m \text{ for some}^1 m \in \mathbb{Z}$$

We can't automatically divide this by 6, but we can certainly divide through by 2:

$$3 \times 9 = 3 \times 5 + 4m \Longrightarrow 3 \mid 4m \Longrightarrow 3 \mid m \Longrightarrow m = 3l \text{ for some } l \in \mathbb{Z}$$

We may now divide by 3 to correctly conclude

$$9 = 5 + 4l \Longrightarrow 9 \equiv 5 \pmod 4$$

It appears that we were able to divide our original congruence by 6, but at the cost of *dividing the modulus* by 2: it just so happens that $2 = \gcd(6, 8)$...

Theorem 3.9. *If $k = 0$ and $\gcd(k, n) = d$, then*

$$ka \equiv kb \pmod n \Longrightarrow a \equiv b \pmod{\tfrac{n}{d}}$$

Proof. $\gcd(k, n) = d \Longrightarrow \gcd\left(\tfrac{k}{d}, \tfrac{n}{d}\right) = 1$ so that $\tfrac{n}{d}$ and $\tfrac{k}{d}$ are *coprime integers.* Appealing to a corollary[2] of Bézout's identity, we see that

$$ka \equiv kb \Longrightarrow n \mid (ka - kb) \Longrightarrow \frac{n}{d} \mid \frac{k}{d}(a - b) \Longrightarrow \frac{n}{d} \mid (a - b)$$

Otherwise said $a \equiv b \pmod{\tfrac{n}{d}}$. ∎

Examples 3.10. 1. We divide by 4 in the congruence $12 \equiv 28 \pmod 8$. Since $\gcd(4, 8) = 4$ we also divide the modulus by 4 to obtain

$$12 \equiv 28 \pmod 8 \Longrightarrow 3 \equiv 7 \pmod 2$$

2. We divide by 12 in the congruence $12 \equiv 72 \pmod{30}$. Since $\gcd(12, 30) = 6$, we conclude that

$$12 \equiv 72 \pmod{30} \Longrightarrow 1 \equiv 6 \pmod 5$$

.

Division in the ring $\mathbb{Z}_n$ The development of modular arithmetic (Theorem 3.6) shows that the set of residues $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ modulo n has the algebraic structure of a *ring*.[3] The interesting question for us is when one can *divide.*

Recall in the real numbers that to divide by x means that we *multiply* by some element x^{-1} satisfying $xx^{-1} = 1$: plainly this is possible provided $x \neq 0$. The same idea holds in $\mathbb{Z}_n$.

Definition 3.11. Let $x \in \mathbb{Z}_n$. We say that $y \in \mathbb{Z}_n$ is the *inverse* of x if $xy \equiv yx \equiv 1 \pmod{n}$.
An element x is a *unit* if it has an inverse. A ring is a *field* if every non-zero element is a unit.

Example 3.12. By considering the multiplication tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$, we can easily identify the units and their inverses:

$\mathbb{Z}_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

There are plainly only *two* units in $\mathbb{Z}_6$, namely 1 and 5. Moreover, each is its own inverse

$$1 \cdot 1 \equiv 1, \quad 5 \cdot 5 \equiv 1 \pmod{6}$$

Modulo 5, however, every non-zero residue is a unit:

$$1 \cdot 1 \equiv 1, \quad 2 \cdot 3 \equiv 3 \cdot 2 \equiv 1, \quad 4 \cdot 4 \equiv 1 \pmod{5}$$

In the example, the units have a simple property in common.

Theorem 3.13. *$x \in \mathbb{Z}_n$ is a unit $\iff \gcd(x, n) = 1$.*
Moreover, every non-zero $x \in \mathbb{Z}_n$ is a unit (thus $\mathbb{Z}_n$ is a field*) if and only if $n = p$ is* prime.

Proof. ($\Rightarrow$) If $xy \equiv 1 \pmod{n}$, then $xy - \lambda n = 1$ for some $\lambda \in \mathbb{Z}$. Plainly any common factor of x and n divides 1, whence $\gcd(x, n) = 1$.

($\Leftarrow$) By Bézout's identity, $\exists \lambda, y \in \mathbb{Z}$ such that

$$xy + n\lambda = 1 \implies xy \equiv 1 \pmod{n}$$

Plainly every non-zero x is a unit if and only if $\gcd(x, n) = 1$ for all $x \in \{1, \ldots, n-1\}$. This is if and only if n has no divisors except itself and 1: i.e. n is prime. ∎

This result gels with Theorem 3.9: we can divide a congruence by k *while remaining in* $\mathbb{Z}_n$ precisely when $d = \gcd(k, n) = 1$. Moreover, the proof tells us how to compute inverses:

.

Example 3.14. Find the inverse of $15 \in \mathsf{Z}_{26}$.

First observe that $\gcd(15, 26) = 1$, so an inverse exists. Now apply the Euclidean algorithm and Bézout's identity:

$$\begin{aligned} \mathbf{26} &= 1 \cdot \mathbf{15} + \mathbf{11} \qquad \Longrightarrow \gcd(26, 15) = \mathbf{1} = \mathbf{4} - \mathbf{3} = \mathbf{4} - (\mathbf{11} - 2 \cdot \mathbf{4}) \\ \mathbf{15} &= 1 \cdot \mathbf{11} + \mathbf{4} \qquad\qquad\qquad\quad = 3 \cdot \mathbf{4} - \mathbf{11} = 3(\mathbf{15} - \mathbf{11}) - \mathbf{11} \\ \mathbf{11} &= 2 \cdot \mathbf{4} + \mathbf{3} \qquad\qquad\qquad\quad = 3 \cdot \mathbf{15} - 4 \cdot \mathbf{11} = 3 \cdot \mathbf{15} - 4(\mathbf{26} - \mathbf{15}) \\ \mathbf{4} &= 1 \cdot \mathbf{3} + \mathbf{1} \qquad\qquad\qquad\quad = 7 \cdot \mathbf{15} - 4 \cdot \mathbf{26} \end{aligned}$$

from which we see that $15 \cdot 7 \equiv 1 \pmod{26}$: the inverse of 15 is therefore 7.

Exercises 3.1 1. Find the residues (remainders) of the following expressions:

(a) $6^4 - 38 \cdot 48 \pmod 5$

(b) $117^{32} + 118^{31} \pmod 7$

(c) $3510^{1340} - 2709^{4444} \pmod{24}$

2. Suppose that $d \mid m$. Show that if $a \equiv b \pmod{\frac{m}{d}}$, then

$$a \equiv b, \quad \text{or} \quad b + \frac{m}{d}, \quad \text{or} \quad \cdots, \quad \text{or} \quad b + (d-1)\frac{m}{d} \pmod m$$

3. Show that a positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

(*Hint: for example* $471 = 4 \cdot 100 + 7 \cdot 10 + 1 \ldots$)

4. Suppose $z \in \mathsf{N}$ and that $z \equiv 3 \pmod 4$. Prove that at least one of the primes p dividing z must be congruent to 3 modulo 4.

5. (a) State the units in the ring Z_{48}.

(b) Find the inverse of 11 modulo 48.

(c) If $11x \equiv 2 \pmod{48}$ for some $x \in \mathsf{Z}_{48}$, find x.

6. Prove that inverses are unique: if y, z are inverses of $x \in \mathsf{Z}_n$, then $y \equiv z \pmod n$.

7. A non-zero element $x \in \mathsf{Z}_n$ is a *zero divisor* if $\exists y \in \mathsf{Z}_n$ such that $xy \equiv 0 \pmod n$. Prove that Z_n has zero divisors if and only if n is composite.

8. Suppose p is prime and $a \not\equiv 0$. Prove that the remainders $0, a, 2a, 3a, \ldots, (p-1)a$ are *distinct* modulo p, and thus constitute all of Z_p.

9. Suppose r and s are odd. Prove the following:

(a) $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} \pmod 2$

(b) $r^2 \equiv s^2 \equiv 1 \pmod 8$

(c) $\frac{(rs)^2 - 1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} \pmod 8$

10. Prove that (k^k) is periodic modulo 3 and find its period.

(*Hint: First try to spot a pattern...*)

3.2 Congruence Equations and Lagrange's Theorem

In this section we consider polynomial congruence equations $p(x) \equiv 0 \pmod{m}$. The simplest type are *linear*: in fact we know how to solve these already.

$$\exists x \in \mathbb{Z} \text{ s.t. } ax \equiv c \pmod{m} \iff \exists x, y \in \mathbb{Z} \text{ s.t. } ax + my = c$$

This last is a linear Diophantine equation; we need only rephrase our work from earlier.

Theorem 3.15. *Let $d = \gcd(a, m)$. The equation $ax \equiv c \pmod{m}$ has a solution iff $d \mid c$. If x_0 is a solution, then all solutions are given by*

$$x = x_0 + k\frac{m}{d} : k \in \mathbb{Z}$$

Moreover, modulo m, there are exactly d solutions, namely

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d},\ \ldots, x_0 + \frac{(d-1)m}{d}$$

Examples 3.16. 1. We solve the congruence equation $15x = 4 \pmod{133}$.

By the Euclidean algorithm/Bézout, we see that

$$\begin{aligned} \mathbf{133} &= 8 \cdot \mathbf{15} + \mathbf{13} \\ \mathbf{15} &= 1 \cdot \mathbf{13} + \mathbf{2} \\ \mathbf{13} &= 6 \cdot \mathbf{2} + \mathbf{1} \end{aligned} \qquad \Rightarrow d = \gcd(15, 133) = \mathbf{1} = \mathbf{13} - 6 \cdot \mathbf{2} = \mathbf{13} - 6(\mathbf{15} - \mathbf{13})$$
$$= 7 \cdot \mathbf{13} - 6 \cdot \mathbf{15}$$
$$= 7(\mathbf{133} - 8 \cdot \mathbf{15}) - 6 \cdot \mathbf{15}$$
$$= 7 \cdot \mathbf{133} - 62 \cdot \mathbf{15}$$

Since $d = 1$ and $d \mid 4$, there is exactly one solution. Moreover, modulo 133, we see that

$$15 \cdot (-62) \equiv 1 \Rightarrow 15 \cdot (-248) \equiv 15 \cdot 18 \equiv 4 \pmod{133}$$

whence $x_0 = 18$ is the unique solution.[a]

2. We solve the linear congruence $1288x \equiv 21 \pmod{1575}$.
Assume we have applied the Euclidean algorithm and Bézout's identity to obtain

$$d = \gcd(1575, 1288) = 7 = 1575 \cdot 9 - 1288 \cdot 11$$

Since $7 \mid 21$, there are precisely *seven* solutions. Indeed

$$7 \equiv 1288(-11) \pmod{1575} \Rightarrow x = -33 \equiv 1542 \pmod{1575}$$

Moreover, $\frac{m}{d} = \frac{1575}{7} = 225$, whence all solutions are

$$\{x \equiv -33 + 225k : k = 0, \ldots, 6\} = \{192, 417, 642, 867, 1092, 1317, 1542\}$$

Higher degree congruences : While we were able to give a complete description of the solutions to a linear congruence, for higher order polynomials, things quickly become very messy. We start with a simple example of a quadratic congruence which can easily be solved by inspection.

Example 3.17. Consider the quadratic equation $x^2 + 3x \equiv 0 \pmod{10}$. One can easily check by plugging in the remainders $0, \ldots, 9$ that the solutions to this equation are

$$x \equiv 0, 2, 5, 7 \pmod{10}$$

This is perhaps surprising, since we are used to quadratic equations having at most *two* solutions.

Now consider the same equation modulo the prime divisors of 10. Since $10 \mid d \iff 2 \mid d$ and $5 \mid d$, we see that

$$x^2 + 3x \equiv 0 \pmod{10} \iff \begin{cases} x^2 + 3x \equiv 0 \pmod{2} \\ x^2 + 3x \equiv 0 \pmod{5} \end{cases}$$

By substituting values for x, we easily check that sanity is restored: each congruence now has two solutions!

$$x^2 + 3x \equiv 0 \pmod{2} \iff x \equiv 0, 1 \pmod{2}$$
$$x^2 + 3x \equiv 0 \pmod{5} \iff x \equiv 0, 2 \pmod{5}$$

We can even factorize in the familiar manner:

$$x^2 + 3x \equiv x^2 - x \equiv x(x-1) \pmod{2}$$
$$x^2 + 3x \equiv x^2 - 2x \equiv x(x-2) \pmod{5}$$

Modulo 10, however, we have two distinct factorizations:

$$x^2 + 3x \equiv x(x-7) \equiv (x-2)(x-5) \pmod{10}$$

For general polynomial congruences, the same sort of thing is true. The number of solutions and types of factorizations are more predictable when the modulus is *prime*.

Theorem 3.18 (Lagrange). *Let p be prime and $f(x)$ a polynomial with integer coefficients and degree n modulo p. Then $f(x) \equiv 0 \pmod{p}$ has at most n distinct roots.*

Lagrange's Theorem is useless for congruences such as $x^{39} + 25x^2 + 1 \equiv 0 \pmod{17}$: since there are only 17 distinct values of x to try, the congruence has a maximum of 17 solutions, not 39.

Before proving Lagrange's Theorem, we need one additional ingredient.

Lemma 3.19 (Factor Theorem in $\mathbb{Z}[x]$). *Suppose $f(x)$ is a polynomial with integer coefficients and that $c \in \mathbb{Z}$. Then there exists a unique polynomial $q(x)$, also with integer coefficients, such that*

$$f(x) = (x-c)q(x) + f(c)$$

Moreover, $f(c) = 0$ if and only if $(x-c)$ is a factor of $f(x)$. This is also true modulo any *n.*

Proof of Lagrange. Suppose $f(x) = a_n x^n + \cdots$ is a polynomial with integer coefficients and degree n modulo p: that is, $p \nmid a_n$. Moreover, assume that $f(c_1) \equiv 0 \pmod{p}$. By the factor theorem, there exists a unique polynomial $q_1(x)$ with integer coefficients, such that

$$f(x) = (x - c_1)\, q_1(x) + f(c_1) \equiv (x - c_1)\, q_1(x) \pmod{p}$$

Plainly $q_1(x) = a_n x^{n-1} + \cdots$ has degree $n - 1$ modulo p. If $c_2 \not\equiv c_1$ is another root modulo p, then

$$0 \equiv f(c_2) \equiv (c_2 - c_1) q_1(c_2) \implies q_1(c_2) \equiv 0 \pmod{p}$$

The last step is where we need p to be prime.[4] We may therefore factor out $(x - c_2)$ from $q_1(x)$ modulo p, and thus from $f(x)$. Repeating the process, if there are n distinct roots, then $f(x)$ factorizes as

$$f(x) \equiv (x - c_1) \cdots (x - c_n) q_n(x) \pmod{p}$$

where $q_n(x)$ has degree $n - n = 0$: it is necessarily the constant a_n. Finally, if $\xi \not\equiv c_i$ for any i, then

$$f(\xi) \equiv a_n (\xi - c_1) \cdots (\xi - c_n) \not\equiv 0 \pmod{p}$$

since there are no zero divisors in $\mathbb{Z}_p$. We conclude that $f(x) \equiv 0$ has no further roots modulo p. ∎

In fact the ring of polynomials with coefficients in $\mathbb{Z}_p$ has a Euclidean algorithm which can be used to prove a unique factorization theorem: there is only one way to factorize a polynomial modulo p. We won't prove it, but you are welcome to use the fact nonetheless