

Number Theory

Vinesh Ramgi

March 24, 2018

Contents

1	Introduction/Review	3
1.1	Introduction	3
1.2	Review	3
1.2.1	Congruences	3
1.2.2	Solving Linear Congruences	4
1.3	Chinese Remainder Theorem	5
1.4	Prime numbers	7
1.5	Fermat's Little Theorem	7
1.5.1	General method to solve $x^a \equiv b \pmod{p}$	8
1.6	Fundamental Theorem of Arithmetic	8
1.6.1	Euclid's Lemma	8
1.6.2	Checking whether a number is prime	9

1 Introduction/Review

1.1 Introduction

Number Theory is the theory of the ring \mathbb{Z} and other related rings. A ring (in this course) is a set R with two binary operations $+$ and $*$ such that:

- $(R, +)$ is an abelian group
- $*$ is associative, commutative and has an identity element 1
- $x(y + z) = xy + xz \quad \forall x, y, z \in R$

Examples of rings:

- \mathbb{Z} is a ring
- Every field is a ring, (e.g. $\mathbb{R}, \mathbb{C}, \mathbb{Q}$)
- \mathbb{Z}/n \mathbb{Z} modulo $n = \{0, \dots, n-1\}$
- $\mathbb{F}[X] = \{ \text{polynomials } f(x) \text{ with coefficients in } \mathbb{F} \}$

1.2 Review

1.2.1 Congruences

Let n be a positive integer. Given $x, y \in \mathbb{Z}$, we say x is congruent to y modulo n if $x - y$ is a multiple of n .

$$x \equiv y(n) \quad \text{or} \quad x \equiv y \pmod{n}$$

E.g $2 \equiv 12 \pmod{10}$
 $\equiv -8 \pmod{10}$

We write \mathbb{Z}/n for the ring of congruency classes modulo n , i.e. the elements are integer, with two of them regarded as the same if they are congruent modulo n .

Since every integer is congruent to a unique integer in the set $\{0, \dots, n-1\}$, we have $\mathbb{Z}/n = \{0, \dots, n-1\}$.

An element x of \mathbb{Z}/n is called "invertible" or a "unit" if $\exists y \in \mathbb{Z}/n$ such that $xy \equiv 1(n)$.

Theorem 1.1. x is invertible modulo n iff x and n are coprime

Recall Two numbers are coprime if their highest common factor is 1.

Here's how we find the inverse of x in \mathbb{Z}/n . Since X and n are coprime we can find $h, k \in \mathbb{Z}$ such that $hx + kn = 1 \implies hx \equiv 1 \pmod{n}$. So h is the inverse of x modulo n .

E.g We'll find the inberse of 7 modulo 25 using Euclid's algorithm

$$25 = 3 \times 7 + 4$$

$$7 = 1 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

$$1 = 4 - 1(3)$$

$$1 = 4 - 1(7 - 1(4)) = 2(4) - 1(7)$$

$$1 = 2(25 - 3(7)) - 1(7) = 2(25) - 7(7)$$

$$2(25) - 7(7) = 1$$

$$- 7(7) = 1 \pmod{25}$$

$$(7^{-1}) = -7 = 18 \pmod{25}$$

$$7 \times 18 = 126 = 1 \pmod{25}$$

We'll write $(\mathbb{Z}/n)^\times$ for the invertible elements in \mathbb{Z}/n

E.g

$$(\mathbb{Z}/3)^\times = \{ \emptyset, 1, 2 \}$$

$$(\mathbb{Z}/6)^\times = \{ \emptyset, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5 \}$$

Theorem 1.2. $(\mathbb{Z}/n)^\times$ is a group with the operation of multiplicity.

1.2.2 Solving Linear Congruences

Suppose we want to solve $ax \equiv b \pmod{n}$ (given a, b and n).

Case 1: If a is coprime to n then we can find a^{-1} modulo n by Euclid's algorithm,

$$x \equiv a^{-1}b \pmod{n}$$

Case 2: If a is a factor of n , then there are two possibilities:

2a) if a is also a factor of b then $ax \equiv b \pmod{n}$ is equivalent to $x = \frac{b}{a} \pmod{\frac{n}{a}}$

2b) if a is not a factor of b then there are no solutions

E.g. Solve $5x = 11 \pmod{13}$

This is case 1 because 5 and 13 are coprime

$$13 = 2 \times 5 + 3$$

$$5 = 1 \times 3 + 2$$

$$3 = 1 \times 2 + 1$$

$$1 = (3) - 1(2)$$

$$1 = (3) - 1(5 - 1(3)) = 2(3) - (5)$$

$$1 = 2(13 - 2(5)) - (5) = 2(13) - 5(5)$$

$$1 \equiv -5(5) \pmod{13}$$

$$5^{-1} \equiv -5 \equiv 8 \pmod{13}$$

$$5x \equiv 11 \pmod{13}$$

$$x \equiv 8 \times 11 \equiv 88 \pmod{13}$$

$$x \equiv 10 \pmod{13}$$

E.g. Solve $7x \equiv 84 \pmod{490}$

7 is a factor of 490 so case 2)

7 is a factor of 84 so case 2a)

$$7x \equiv 84 \pmod{490}$$

$$x \equiv 12 \pmod{70}$$

E.g. Solve $7x \equiv 85 \pmod{490}$

This is case 2b (7 is a factor of 490 but not of 85) \therefore No solutions

$$7x \equiv 85 \pmod{490}$$

$$\implies 7x = 85 + 490y \text{ for some } y \in \mathbb{Z}$$

$$\implies 0 \equiv 1 \pmod{7}$$

E.g. Solve $6x \equiv 3 \pmod{21}$

This is neither case 1 nor case 2 but we can rewrite as:

$$3(2x) \equiv 3 \pmod{21}$$

$$\text{By case 2 we can solve for } 2x \equiv 1 \pmod{7}$$

but now 2 is invertible modulo 7 so now solve by case 1

$$\therefore x \equiv 4 \pmod{7}$$

1.3 Chinese Remainder Theorem

Suppose we know the congruency class of x modulo 10. Then we can work out its congruency class mod 2 and mod 5.

E.g. if $x \equiv 7 \pmod{10}$, then $x \equiv 1 \pmod{2}$ and $x \equiv 2 \pmod{5}$

Then the Chinese Remainder Theorem allows us to do the opposite, i.e. if we know x modulo 2 and modulo 5, then we can work out the value of x modulo 10.

Suppose n & m are coprime positive integers, let $a \in (\mathbb{Z}/n)$ and $b \in (\mathbb{Z}/m)$ then there is a unique

$$x \in (\mathbb{Z}/nm) \text{ such that } \begin{aligned} x &\equiv a \pmod{n} \\ x &\equiv b \pmod{m} \end{aligned}$$

Proof of existence part:

Since n & m are coprime, we can find $h, k \in \mathbb{Z}$ such that $hn + km = 1$.

Let $x = hnb + kma$

Check that this a solution to both congruences:

$$\begin{aligned} x &\equiv kma \pmod{n} \\ x &\equiv (1 - hn)a \pmod{n} \\ x &\equiv (1)a \pmod{n} \\ x &\equiv a \pmod{n} \end{aligned}$$

Similarly, this holds for $x \equiv b \pmod{m}$.

E.g. Solve the simultaneous congruence:

$$\begin{aligned} x &\equiv 3 \pmod{8} \\ x &\equiv 4 \pmod{5} \end{aligned}$$

By the Chinese Remainder Theorem, there is unique solution modulo 40. To find the solution we let $x = hnb + kma$.

First find h, k by Euclid's algorithm.

$$\begin{aligned} 8 &= 1 \times 5 + 3 & 1 &= (3) - 1(2) \\ 5 &= 1 \times 3 + 2 & 1 &= (3) - 1(5 - 1(3)) = 2(3) - (5) \\ 3 &= 1 \times 2 + 1 & 1 &= 2(8 - 2(5)) - (5) = 2(8) - 5(5) \end{aligned}$$

$$\begin{aligned} \therefore x &= (2 * 8 * 4) - (3 * 5 * 3) \\ x &= 64 - 45 \\ \implies x &\equiv 19 \pmod{40} \end{aligned}$$

Remark: We can use the Chinese Remainder Theorem to solve a congruence modulo nm , by first solving mod n and then mod m and then combining the results.

E.g. Solve $x^2 \equiv 2 \pmod{119}$. Note $119 = 7 * 17$.

By CRT this is equivalent to:

$$\begin{aligned} x^2 &\equiv 2 \pmod{7} & \implies x &\equiv \pm 3 \pmod{7} \\ x^2 &\equiv 2 \pmod{17} & \implies x &\equiv \pm 6 \pmod{17} \end{aligned}$$

Now we combine the solutions:

$$\begin{aligned} 17 &= 2 * 7 + 3 & 1 &= (7) - 2(3) \\ 7 &= 2 * 3 + 1 & 1 &= (7) - 2(17 - 2(7)) \\ & & 1 &= 5(7) - 2(17) \end{aligned}$$

Since

$$\begin{array}{ll} x \equiv \pm 3 \pmod{7} & \text{We get } x \equiv 5 * 7 * (\pm 6) - 2 * 17 * (\pm 3) \\ x \equiv \pm 6 \pmod{17} & x \equiv \pm 11 \text{ or } \pm 45 \pmod{119} \end{array}$$

1.4 Prime numbers

Defintion 1.3. An integer $p \geq 2$ is a prime number if the only factors of p are $\pm 1, \pm p$

We'll write \mathbb{F}_p for \mathbb{Z}/p . This is because:

Theorem 1.4. If p is prime, then \mathbb{F}_p is a field

Proof. Need to check that the non-zero elements of \mathbb{F}_p all have inverses.

Let $x \in \mathbb{F}_p$ with $x \not\equiv 0 \pmod{p}$ i.e. x is not a multiple of p

$$\therefore \text{hcf}(x, p) = 1$$

$\therefore x$ & p coprime □

1.5 Fermat's Little Theorem

Theorem 1.5. Let p be a prime number. If x is not a multiple of p then $x^{p-1} \equiv 1 \pmod{p}$

Proof. $x \in \mathbb{F}_p^\times = \{1, 2, \dots, p-1\}$ a group with $p-1$ elements.

Let n be the order of x in this group.

(order of x is smallest $n > 0$ such that $x^n \equiv 1 \pmod{p}$)

By corollary to Lagrange's Theorem, $p-1$ is a multiple of n

$$\begin{array}{l} x^n \equiv 1 \pmod{p} \\ x^{p-1} \equiv 1 \pmod{p} \end{array} \quad \square$$

Theorem 1.6. Lagrange's Theorem: If H is a subgroup of a finite group G , then $|H|$ is a factor of $|G|$.

Corollary 1.7. Order of an element is a factor of $|G|$

We can use Fermat's Little Theorem to do calculations.

E.g. Calculate 10^{100} modulo 19

By Fermat's Little Theorem: $10^{18} \equiv 1 \pmod{19}$

$$\begin{aligned} 10^{100} &\equiv (10^{18})^5 * 10^{10} \pmod{19} \\ &\equiv 100^5 \pmod{19} \\ &\equiv 5^5 \pmod{19} \\ &\equiv 25 * 125 \equiv 6 * 11 \equiv 9 \pmod{19} \end{aligned}$$

Also using Fermat's Little Theorem we can solve congruence of the form $x^a \equiv b \pmod{p}$ as long as p prime and a invertible modulo $p-1$

1.5.1 General method to solve $x^a \equiv b \pmod{p}$

Let

$$\begin{aligned}c &= a^{-1} \pmod{p-1} \\ac &= 1 + (p-1)r\end{aligned}$$

Raise both sides of the congruence to power c :

$$\begin{aligned}\therefore x^{ac} &\equiv b^c \pmod{p} \\x^{1+(p-1)r} &\equiv b^c \pmod{p} \\x &\equiv b^c\end{aligned}$$

So the solution is $x \equiv b^c \pmod{p}$

E.g. Solve $x^5 \equiv 2 \pmod{19}$

19 is prime and 5 is coprime to 18.

Find $c = 5^{-1} \pmod{18}$

$$\begin{array}{ll}18 = 3 * 5 + 3 & 1 = 2 * 3 - 5 \\5 = 2 * 3 - 1 & 1 = 2(18 - 3 * 5) - 5 \\& 1 = 2 * 18 - 7 * 5\end{array}$$

$$\begin{aligned}\therefore 5^{-1} &\equiv -7 \pmod{18} \\&\equiv 11 \pmod{18}\end{aligned}$$

$$\begin{aligned}\therefore x &\equiv 2^{11} \pmod{19} \\&\equiv 2048 \pmod{19} \\&\equiv 15 \pmod{19}\end{aligned}$$

1.6 Fundamental Theorem of Arithmetic

If n is a positive integer then there is a unique factorisation, $n = p_1 p_2 \dots p_r$ with p_i prime. "Unique" means up to reordering the primes p_1, \dots, p_r . Showing that a factorisation exists is easy. For the uniqueness part we use:

1.6.1 Euclid's Lemma

Lemma 1.8. Suppose p prime, and $p|ab$. Then $p|a$ or $p|b$.

To prove Euclid's lemma we use Bezout's lemma.

Proof. Assume $p|ab$ but $p \nmid a$. Then $\text{hcf}(a, p) = 1$

By Bezout's lemma, $\exists h, k$ such that:

$$1 = ha + kp$$

$$b = hab + kpb$$

Both hab and kpb are multiples of p .

$\therefore p|b$

□

1.6.2 Checking whether a number is prime

If n is composite then the smallest factor of n is (apart from 1) is a prime number $p \leq \sqrt{n}$, i.e. to show that n is prime, we just need to show that none of the primes up to \sqrt{n} are factors of n .

E.g. Is 199 prime?

$$\sqrt{199} < 15 \text{ since } 15^2 = 225$$

The primes up to 15 are