Euclidean division, solving linear congruences and structure of the residue class ring $\mathbb{Z}_n$

Virendra Sule
Dept. of EE
IIT Bombay

August 31, 2020

1 Euclidean division in $\mathbb{Z}$

Euclidean division by integers leads to the fact (prove): Given a, b in $\mathbb{Z}$, $b > 0$ there exist unique integers q, r with properties 1) $0 \leq r < b$ and 2) $a = qb + r$. Moreover $q = \lfloor a/b \rfloor$ the integer lower bound of the rational number a/b called *quotient* while r is called the *reminder* and is denoted as $r = a \mod b$. If $a \mod b = 0$ then b is a *divisor* of a (positive by definition) and b divides a is denoted as $b|a$. The *greatest common divisor* of two integers a, b denoted $\gcd(a, b)$ is a common divisor of a, b such that if c is a common divisor then $c|d$. Let the set of all integral linear combinations of a, b, $\{\mathbb{Z}a + \mathbb{Z}b\} = \{ax + by, x, y \in \mathbb{Z}\}$ be denoted $I(a, b)$, $(a) = \{\mathbb{Z}a\}$ denotes all integer multiples of a and $d = \gcd(a, b)$. Then

Theorem 1. $I(a, b) = (d)$

Proof: Write the proof as exercise. This is discussed in the text book. Show that d the gcd of a, b is the minimum positive element of $I(a, b)$.

Euclidean division formula and the gcd has many far reaching consequences in the theory of numbers. Some of the basic facts are as follows. A common notation for the gcd d of a, b is (a, b)

1. If $d = (a, b)$, then there exist integers x, y such that $d = ax + by$.
2. a, b are called *coprime* if $I(a, b) = \mathbb{Z}$ or equivalently $d = 1$. If a, b are coprime then there exist integers x, y such that $ax + by = 1$.
3. The linear equation $ax + by = n$, a, b, n integers has integer solutions x, y iff $d|n$.

More generally, observe that if $a_i, i = 1, ..m$ are integers, using the recursive expression

$$d = \gcd(a_1, \ldots, a_m) = (a_1, (a_2, \ldots, a_m))$$

it follows that the $\mathbb{Z}$-linear span

$$I(a_1, \ldots, a_m) = (d)$$

1.1 The ring of residues $\mathbb{Z}_n$

Let n be a positive integer. The set of reminders (also called residues) $\{r = a \mod n, a \in \mathbb{Z}\}$ equals $\{0, 1, 2, \ldots, (n-1)\}$. The set of integers $\{r + n\mathbb{Z}\}$ consisting of all integers with reminder r called the residue class of r is denoted $[r]$. Call two integers a, b equivalent modulo n if $a - b = 0 \mod n$ i.e. both a, b have the same residue r. This is an equivalence relation on $\mathbb{Z}$ and hence partitions $\mathbb{Z}$ into disjoint equivalence classes $[r]$. The set of all such residues is made into a ring $\mathbb{Z}_n$ with operations

1. addition $[r] \boxplus [s] = [r + s \mod n]$
2. multiplication $[r] \bigodot [s] = [rs \mod n]$

together with the identitiy [1] and additive zero [0] (we now drop the special symbols for addition and multiplication and denote them by usual $+, .$. What are the *units* (the invertible elements) of this ring? By definition r is invertible if there exists s such that $rs = 1$ in this ring i.e. $rs = 1 \mod n$. Hence r is invertible iff there exists integer y such that $rs = 1 + ny$ and by the above theorem it follows that r is invertible iff 1 belongs to (r, n) i.e. $(r, n) = 1$.

1.1.1 Euler's Totient function

The set of units of $\mathbb{Z}_n$ the invertible elements is denoted by $\mathbb{Z}_n^*$ and is a finite *group* under the muliplication operation (prove). (note that the units of $\mathbb{Z}_n$ are nonzero numbers $< n$ and coprime to n. The cardinality $|\mathbb{Z}_n^*|$ is a function of n called *Euler totient function* denoted $\phi(n)$. Observe that $n = p$ is prime iff all nonzero r in $\mathbb{Z}_n$ are coprime to n. This ring $\mathbb{Z}_p$ has all nonzero elements invertible and is thus a finite field called *prime field* field with p elements (also denoted by $\mathbb{F}_p$ or $GF(p)$ called Galoise field). It follows that $\phi(p) = p - 1$. There is a nice formula

Theorem 2. If n is a positive integer

$$\sum_{d|n} \phi(d) = n$$

As an example consider $n = 30$. The divisors of n are $\{1, 2, 3, 5, 6, 10, 15, 30\}$. We can observe that $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(5) = 4$, $\phi(6) = 2$, $\phi(10) = 4$, $\phi(15) = 8$, $\phi(30) = 8$. The sum is $1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30$. See the proof in the text book [1]. We will see more properties of the Euler function later.

1.2 Relations with groups theory

Read about the definition of a *group* and a *subgroup* from the Buchmann's text or from any other basic text. Prove that the set $\mathbb{Z}_n^*$ is a group under the product operation. This is also an Abelian group as the product operation is commutative. Well known examples of non-Abelian (or non-commutative) groups are group of permutations of n objects denoted S_n also called the symmetric group and the group of nonsingular $n \times n$ matrices over a field F denoted $GL(n, F)$ called the general linear group over F. We shall mostly consider finite groups.

1.2.1 Lagrange's theorem

Let G be a finite group and H be a subgroup. An example of a subgroup in G is the cyclic group generated by powers of one element $\{g^k, k \in \mathbb{Z}\}$ in G and denoted $< g >$. H may be generated by more elements such as $\{g^k h^l, g, h \in G, k, l \in \mathbb{Z}\}$. For a in G and a subgroup H consider the set $\{aH\} = \{ah, h \in H\}$. Two elements a, b in G are said to be equivalent modulo H if ab^{-1} is in H. Show that this is an equivalence relation in G and $\{aH\}$ are equivalence classes which thus partition G. Observe that if h, h' are in H and $ah = ah'$ then pre-multiplying by a^{-1} we get $h = h'$. Hence all elements of aH are distinct and $|\{aH\}| = |H|$ for any a in G. hence it follows that $|G|$ is a multiple of $|H|$ the ratio $(G : H) = |G|/|H|$ is called the *degree* of H in G. (The fact that $|H|$ divides $|G|$ is known as Lagrange's theorem). If g is in G the smallest positive integer e such that $g^e = 1$ is called the order of g in G denoted $\mathrm{ord}_G g$ or simply $\mathrm{ord}\, g$. $|G|$ is called the order of G denoted $\mathrm{ord}\, G$. The smallest positive integer α such that $g^\alpha = 1$ for all g in G is called the *index* of G.

Following facts follow from the Lagrange's theorem (that the order of a subgroup divides the order of the group).

1. Since $< g >$ is a cyclic subgroup of G, if e is order of g, then $e||G|$ for any element g. Hence $g^{|G|} = 1$ for any g.

2. **Euler's theorem** If a, n are coprime, then $a^{\phi(n)} \mod n = 1$. (follows from the fact that $r = a \mod n$ is an element of $\mathbb{Z}_n^*$ if a, n are coprime and hence $r^{\phi(n)} = 1$ in $\mathbb{Z}_n^*$ as $\phi(n)$ is the order of $\mathbb{Z}_n^*$.

3. **Fermat's little theorem** If p is prime and a is not divisible by p then $a^{p-1} = 1 \mod p$. (Apply above for $\mathbb{Z}_p^*$).

2 Extended Euclidean algorithm and solving linear equations

The Euclidean algorithm can be used to compute integers x, y such that $ax + by = d$ where $d = \gcd(a, b)$. Consider the problem of solving the equation

$$aX + bY = n$$

for integers X, Y. From theorem 1, this equation has a solution x, y iff $d|n$ where d is the $\gcd(a, b)$. So let $n = n'd$, $a = a'd$, $b = b'd$ and let x, y be one solution of $ax + by = d$ obtained using the extended Euclidean algorithm. We thus equivalently have $a'x + b'y = 1$. If x', y' are any other solutions of $ax + by = d$ then $a'(x - x') + b'(y - y') = 0$. Since a', b' are now coprime it follows that $(x - x') = -b'r$ and $(y' - y) = a'r$ for any integer r. Hence all such solutions are

$$x' = x + b'r,\ y' = y + a'r$$

Since $a'x + b'y = 1$ multiplying by n we get all solutions of the above equation as

$$X = n'(x + b'r),\ Y = n'(y - a'r)$$

2.1 Solving congruences

Consider now the problem of solving the congruences of the type

$$aX = b \mod n,$$

This has a solution x iff $ax - b = ny$ for some y. Hence this problem reduces to solving the equation $aX - nY = b$ which is same as above. The solution exists iff $d|b$ where $d = \gcd(a, n)$. Let $a = da'$, $n = dn'$, $b = db'$ and let x, y be any solutions such that $a'x + n'y = 1$. Then all solutions are

$$X = b'(x + n'r)$$

where r is any integer. Exercise: verify that $aX = b \mod n$.

3 Chinese reminder theorem and the structure of $\mathbb{Z}_n$

Let m, n be coprime integers. Consider the problem of solving the simultaneous congruences

$$\begin{aligned} X &= a \mod m \\ X &= b \mod n \end{aligned}$$

Clearly $x = a + rm$, for integers r are all solutions of the first. Hence second congruence is satisfied when $a + rm = b \mod n$ i.e. there exist integers r, s such that $a - b = ns - mr$. Hence as seen above a solution exists iff $\gcd(m, n)|(a - b)$. This is satisfied since m, n are coprime. Let x, y be a solution of $mx + ny = 1$. Thus $mx = 1 \mod n$ and $ny = 1 \mod m$ hence $mxb + nya = a \mod m$ and $mxb + nya = b \mod n$. Now consider the set of all integers

$$\{(mx'b + ny'a)\}$$

where x', y' are arbitrary solutions in $mx' + ny' = 1$. All solutions of this equation are $x' = (x + nr)$,$y' = (y - mr)$ for any integer r. Hence $(mx'b + ny'a) \mod mn = (mxb + nya) \mod mn$. Hence modulo mn there is a unique solution to the congruences. This proves the CRT in two case. More generally.

Theorem 3 (Chinese Reminder Theorem (CRT))**.** Let $m_1, m_2, \ldots, m_k$ be pairwise coprime integers. Then there is a unique solution in $\mathbb{Z}_m$ to the congruences

$$X = a_i \mod m_i,\ i = 1, 2, \ldots, k$$

where $m = m_1 m_2 \ldots m_k$.

Proof: Read the proof from the book which is a direct generalization of the proof of the two case above.

3.1 Group and ring Homomorphisms

Let G, H be two groups. A function $f : G \to H$ is called a homomorphism of groups if $f(ab) = f(a)f(b)$ for a, b in G. Hence if e is the group identity then $f(e) = e$ (the identiy in H) and $f(a^{-1} = f(a)^{-1}$. f is *injective* if $f(a) = e$ implies $a = e$. f is *surjective* if

$F(G) = H$. G, H are said to be *isomorphic* if there is a homomorphism between them which injective and surjective (called an isomorphism). For rings we have analogous ring homomorphism. If R, S are rings a function $f : R \to S$ is called a *homomorphism* of the rings if $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$. Thus $f(0) = 0$ and if e is the multiplicative identity of R then $f(e)$ is the multiplicative identity of S. If a is a unit of R then $f(a)$ is a unit of S and $f(a^{-1}) = f(a)^{-1}$. A homomorphism f is said to be *injective* if $f(a) = 0$ implies $a = 0$ and *surjective* if $S = f(R)$. An *isomorphism* of rings is an injective and surjective homomorphism. If such exists the rings are called isomorphic.

3.1.1 Structure of $\mathbb{Z}_m$ and $\mathbb{Z}_m^*$

Given pairwise coprime integers m_i as above and m their product, CRT leads to understanding of the structure of the ring $\mathbb{Z}_m$ and the group $\mathbb{Z}_m^*$. Consider the rings $R_i = \mathbb{Z}_{m_i}$ and groups $G_i = \mathbb{Z}_{m_i}^*$ and their direct products

$$R = R_1 \times R_2 \times \ldots \times R_k$$

which is a ring of k-tuples with i-th component in R_i and sum product defined by

$$\begin{aligned} (a_1, \ldots, a_k) + (b_1, \ldots, b_k) &= (a_1 + b_1, \ldots, a_k + b_k) \\ (a_1, \ldots, a_k)(b_1, \ldots, b_k) &= (a_1 b_1, \ldots, a_k b_k) \end{aligned}$$

(what are the identity and 0 element of R?)

$$G = G_1 \times G_2 \times \ldots \times G_k$$

which is a group under the group operation of multiplication same as multiplication defined for the ring elements. What are identity and inverse in this group?

The CRT is equivalent to the theorem

Theorem 4.

$$\begin{aligned} \mathbb{Z}_m &\cong \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \\ \mathbb{Z}_m^* &\cong \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_k}^* \end{aligned}$$

Since there is a unique solution modulo m to the congruences $X = a_i \mod m_i$, for any such solution a there is unique $a \mod m$ in $\mathbb{Z}_m$ for which $a_i = a \mod m_i$. Hence proof follows from the homomorphism (verify that this is a homomorphism)

$$f(a \mod m) = (a_1, a_2, \ldots, a_k)$$

which is both injective and surjective (verify these properties).

3.2 Computation of the Euler phi

Due to the isomorphism of groups $\mathbb{Z}_m^*$ and the product group $\prod \mathbb{Z}_{m_i}^*$ it follows that the number of elements in both are same. Hence the number of elements of $\mathbb{Z}_m$ coprime to m is equal to the product of number of elements in $\mathbb{Z}_{m_i}$ coprime to m_i. From this it follows that

Theorem 5. If m, n are coprime then $\phi(mn) = \phi(m)\phi(n)$.

For p prime the formula for $\phi(p^k)$ can be built as follows. Observe that $\mathbb{Z}_m$ for $m = p^k$ consists of integers

$$\{0, 1, 2, \ldots, p^k - 1\}$$

any integer a in this set has a unique expression as

$$a = a_0 + a_1 p + a_2 p^2 + \ldots + a_{k-1} p^{k-1}$$

where a_i can takes values in $\{0, 1, 2, \ldots, p-1\}$. (This is called p-adic expansion of integers). Thus a is coprime to p^k iff $a_0 \neq 0$. Thus each co-efficient a_i for $i > 0$ can take p values while a_0 can take value in $\{1, 2, \ldots, p-1\}$. Hence number of such elements a coprime to p^k is $(p-1)p^{k-1}$. This proves that

$$\phi(p^k) = (p-1)p^{k-1} = (p^k - p^{k-1})$$

From this we get the formula

Theorem 6. If n has prime factorization

$$n = \prod_i p_i^{k_i}$$

then

$$\phi(n) = \prod_i (p^{k_i} - p^{k_i - 1})$$

As a special case if $n = pq$ where p, q are primes then $\phi(n) = (p-1)(q-1)$.

References

[1] Johannes A. Buchmann. Introduction to Cryptography. Springer 2004.

[2] Joseph H. Silverman. A friendly introduction to number theory. Third Edition. Pearson 2006.

[3] Wade TRappe and Lawrence Washington. Introduction to Cryptography and Coding Theory. Pearson Low Price, 2007.

.