Intro to Analysis of Algorithms
Mathematical Foundations
Chapter 9

Michael Soltys

CSU Channel Islands

[**Git** Date:2018-11-20 Hash:f93cc40 Ed:3rd]

Number theory

$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$

$\mathbb{N} = \{0, 1, 2, \dots\}$

We say that x *divides* y, and write $x|y$ if $y = qx$.

If $x|y$ we say that x is *divisor* (also *factor*) of y.

$x|y$ iff $y = \text{div}(x, y) \cdot x$.

We say that a number p is *prime* if its only divisors are itself and 1.

Claim: If p is a prime, and $p|a_1a_2\dots a_n$, then $p|a_i$ for some i.

Proof: It is enough to show that if $p|ab$ then $p|a$ or $p|b$. Let $g = \text{gcd}(a, p)$. Then $g|p$, and since p is a prime, there are two cases.

Case 1, $g = p$, then since $g|a$, $p|a$.

Case 2, $g = 1$, so there exist u, v such that $au + pv = 1$, so $abu + pbv = b$.

Since $p|ab$, and $p|p$, it follows that $p|(abu + pbv)$, so $p|b$.

Fundamental Theorem of Arithmetic

For $a \geq 2$, $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, where p_i are prime numbers, and other than rearranging primes, this factorization is unique.

Proof: We first show the existence of the factorization, and then its uniqueness.

The proof of existence is by complete induction; the basis case is $a = 2$, where 2 is a prime.

Consider an integer $a > 2$; if a is prime then it is its own factorization (just as in the basis case).

Otherwise, if a is composite, then $a = b \cdot c$, where $1 < b, c < a$; apply the induction hypothesis to b and c.

To show uniqueness suppose that $a = p_1 p_2 \dots p_s = q_1 q_2 \dots q_t$ where we have written out all the primes, that is, instead of writing p^e we write $p \cdot p \cdots p$, e times.

Since $p_1 | a$, it follows that $p_1 | q_1 q_2 \dots q_t$. So $p_1 | q_j$ for some j, but then $p_1 = q_j$ since they are both primes.

Now delete p_1 from the first list and q_j from the second list, and continue.

Obviously we cannot end up with a product of primes equal to 1, so the two list must be identical.

Let $m \geq 1$ be an integer. We say that a and b are *congruent modulo m*, and write $a \equiv b \pmod{m}$ (or sometimes $a \equiv_m b$) if $m|(a-b)$.

Another way to say this is that a and b have the same remainder when divided by m; we can say that $a \equiv b \pmod{m}$ if and only if $\mathrm{rem}(m, a) = \mathrm{rem}(m, b)$.

Facts: $a_1 \equiv_m a_2$ and $b_1 \equiv_m b_2$, then $a_1 \pm b_1 \equiv_m a_2 \pm b_2$ and $a_1 \cdot b_1 \equiv_m a_2 \cdot b_2$.

Proposition: If $m \geq 1$, then $a \cdot b \equiv_m 1$ for some b if and only if $\gcd(a, m) = 1$.

Proof: ($\Rightarrow$) If there exists a b such that $a \cdot b \equiv_m 1$, then we have $m|(ab-1)$ and so there exists a c such that $ab - 1 = cm$, i.e., $ab - cm = 1$.

And since $\gcd(a, m)$ divides both a and m, it also divides $ab - cm$, and so $\gcd(a, m)|1$ and so it must be equal to 1.

($\Leftarrow$) Suppose that $\gcd(a, m) = 1$. By the extended Euclid's algorithm there exist u, v such that $au + mv = 1$, so $au - 1 = -mv$, so $m|(au-1)$, so $au \equiv_m 1$. So let $b = u$.

Let $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$.

We call $\mathbb{Z}_m$ the set of integers modulo m.

To add or multiply in the set $\mathbb{Z}_m$, we add and multiply the corresponding integers, and then take the reminder of the division by m as the result.

Let $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | \gcd(a, m) = 1\}$.

$\mathbb{Z}_m^*$ is the subset of $\mathbb{Z}_m$ consisting of those elements which have multiplicative inverses in $\mathbb{Z}_m$.

The function $\phi(n)$ is called the *Euler totient function*, and it is the number of elements less than n that are co-prime to n, i.e., $\phi(n) = |\mathbb{Z}_n^*|$.

If we are able to factor, we are also able to compute $\phi(n)$: suppose that $n = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$, then it is not hard to see that $\phi(n) = \prod_{i=1}^{l} p_i^{k_i - 1}(p_i - 1)$.

Fermat's Little Theorem Let p be a prime number and $\gcd(a, p) = 1$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof: For any a such that $\gcd(a, p) = 1$ the following products

$$1a, 2a, 3a, \ldots, (p-1)a, \tag{1}$$

all taken mod p, are pairwise distinct.

To see this suppose that $ja \equiv ka \pmod{p}$. Then $(j-k)a \equiv 0 \pmod{p}$, and so $p|(j-k)a$.

But since by assumption $\gcd(a, p) = 1$, it follows that $p \not| a$, and so it must be the case that $p|(j-k)$.

But since $j, k \in \{1, 2, \ldots, p-1\}$, it follows that $-(p-2) \leq j - k \leq (p-2)$, so $j - k = 0$, i.e., $j = k$.

Thus the numbers in the list (1) are just a reordering of the list $\{1, 2, \ldots, p-1\}$.

Therefore

$$a^{p-1}(p-1)! \equiv_p \prod_{j=1}^{p-1} j \cdot a \equiv_p \prod_{j=1}^{p-1} j \equiv_p (p-1)!. \tag{2}$$

Since all the numbers in $\{1, 2, \ldots, p-1\}$ have inverses in $\mathbb{Z}_p$, as $\gcd(i,p) = 1$ for $1 \leq i \leq p-1$, their product also has an inverse.

That is, $(p-1)!$ has an inverse, and so multiplying both sides of (2) by $((p-1)!)^{-1}$ we obtain the result.

Exercise: Give a second proof of Fermat's Little theorem using the binomial expansion, i.e., $(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^j y^{n-j}$ applied to $(a+1)^p$.

Group theory

We say that $(G, *)$ is a *group* if G is a set and $*$ is an operation, such that if $a, b \in G$, then $a * b \in G$; this property is called *closure*.

The operation $*$ has to satisfy the following 3 properties:

1. *identity law:* There exists an $e \in G$ such that $e * a = a * e = a$ for all $a \in G$.
2. *inverse law:* For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. This element b is called an *inverse* and it can be shown that it is unique; hence it is often denoted as a^{-1}.
3. *associative law:* For all $a, b, c \in G$, we have $a * (b * c) = (a * b) * c$.

If $(G, *)$ also satisfies the *commutative law*, that is, if for all $a, b \in G$, $a * b = b * a$, then it is called a *commutative* or *Abelian*.

Typical examples of groups are $(\mathbb{Z}_n, +)$ (integers mod n under addition)

$(\mathbb{Z}_n^*, \cdot)$ (integers mod n under multiplication).

Note that both these groups are Abelian.

These are, of course, the two groups of concern for us; but there are many others: $(\mathbb{Q}, +)$ is an infinite group (rationals under addition),

$\mathrm{GL}(n, \mathbb{F})$ (which is the group of $n \times n$ invertible matrices over a field $\mathbb{F}$),

and S_n (the *symmetric group* over n elements, consisting of permutations of $[n]$ where $*$ is function composition).

Exercise: Show that $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n^*, \cdot)$ are groups, by checking that the corresponding operation satisfies the three axioms of a group.

We let $|G|$ denote the number of elements in G (note that G may be infinite, but we are concerned mainly with finite groups).

If $g \in G$ and $x \in \mathbb{N}$, then $g^x = g * g * \cdots * g$, x times.

If it is clear from the context that the operation is $*$, we use juxtaposition ab instead of $a * b$.

Suppose that G is a finite group and $a \in G$; then the smallest $d \in \mathbb{N}$ such that $a^d = e$ is called the *order* of a, and it is denoted as $\mathrm{order}_G(a)$ (or just $\mathrm{order}(a)$ if the group G is clear from the context).

Proposition: If G is a finite group, then for all $a \in G$ there exists a $d \in \mathbb{N}$ such that $a^d = e$. If $d = \mathrm{order}_G(a)$, and $a^k = e$, then $d|k$.

Proof: Consider the list $a^1, a^2, a^3, \ldots$.

If G is finite there must exist $i < j$ such that $a^i = a^j$.

Then, $(a^{-1})^i$ applied to both sides yields $a^{i-j} = e$.

Let $d = \mathrm{order}(a)$ (by the LNP we know that it must exist!).

Suppose that $k \geq d$, $a^k = e$. Write $k = dq + r$ where $0 \leq r < d$.

Then $e = a^k = a^{dq+r} = (a^d)^q a^r = a^r$.

Since $a^d = e$ it follows that $a^r = e$, contradicting the minimality of $d = \mathrm{order}(a)$, unless $r = 0$.

If $(G, *)$ is a group we say that H is a *subgroup* of G, and write $H \leq G$, if $H \subseteq G$ and H is closed under $*$.

That is, H is a subset of G, and H is itself a group.

Note that for any G it is always the case that $\{e\} \leq G$ and $G \leq G$; these two are called the *trivial subgroups* of G.

If $H \leq G$ and $g \in G$, then gH is called a *left coset of G*, and it is simply the set $\{gh | h \in H\}$.

Note that gH is not necessarily a subgroup of G.

Lagrange If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$, i.e., the order of H divides the order of G.

Proof: If $g_1, g_2 \in G$, then the two cosets $g_1 H$ and $g_2 H$ are either identical or $g_1 H \cap g_2 H = \emptyset$.

To see this, suppose that $g \in g_1 H \cap g_2 H$, so $g = g_1 h_1 = g_2 h_2$.

In particular, $g_1 = g_2 h_2 h_1^{-1}$.

Thus, $g_1 H = (g_2 h_2 h_1^{-1}) H$, and since it can be easily checked that $(ab)H = a(bH)$ and that $hH = H$ for any $h \in H$, it follows that $g_1 H = g_2 H$.

Therefore, for a finite $G = \{g_1, g_2, \ldots, g_n\}$, the collection of sets $\{g_1 H, g_2 H, \ldots, g_n H\}$ is a partition of G into subsets that are either disjoint or identical; from among all subcollections of identical cosets we pick a representative, so that $G = g_{i_1} H \cup g_{i_2} H \cup \cdots \cup g_{i_m} H$, and so $|G| = m|H|$, and we are done.

Exercise: Let $H \leq G$. Show that if $h \in H$, then $hH = H$, and that in general for any $g \in G$, $|gH| = |H|$. Finally, show that $(ab)H = a(bH)$.

Exercise: If G is a group, and $\{g_1, g_2, \ldots, g_k\} \subseteq G$, then the set $\langle g_1, g_2, \ldots, g_k \rangle$ is defined as follows

$$\{x_1 x_2 \cdots x_p | p \in \mathbb{N}, x_i \in \{g_1, g_2, \ldots, g_k, g_1^{-1}, g_2^{-1}, \ldots, g_k^{-1}\}\}.$$

Show that $\langle g_1, g_2, \ldots, g_k \rangle \leq G$, and it is called the subgroup *generated* by $\{g_1, g_2, \ldots, g_k\}$. Also show that when G is finite $|\langle g \rangle| = \mathrm{order}_G(g)$.

An example of "reification."

Euler: For every n and every $a \in \mathbb{Z}_n^*$, that is, for every pair a, n such that $\gcd(a, n) = 1$, we have $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof: First it is easy to check that $(\mathbb{Z}_n^*, \cdot)$ is a group.

Then by definition $\phi(n) = |\mathbb{Z}_n^*|$, and since $\langle a \rangle \leq \mathbb{Z}_n^*$, it follows by Lagrange's theorem that $\mathrm{order}(a) = |\langle a \rangle|$ divides $\phi(n)$.

Note that Fermat's Little theorem is an immediate consequence of Euler's theorem, since when p is a prime, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$, and $\phi(p) = (p - 1)$.

Chinese Remainder Given two sets of numbers of equal size, $r_0, r_1, \ldots, r_n$, and $m_0, m_1, \ldots, m_n$, such that

$$0 \leq r_i < m_i \qquad 0 \leq i \leq n \tag{3}$$

and $\gcd(m_i, m_j) = 1$ for $i \neq j$, then there exists an r such that $r \equiv r_i \pmod{m_i}$ for $0 \leq i \leq n$.

Proof: The proof we give is by counting; we show that the distinct values of r, $0 \le r < \Pi m_i$, represent distinct sequences.

To see that, note that if $r \equiv r' \pmod{m_i}$ for all i, then $m_i | (r - r')$ for all i, and so $(\Pi m_i) | (r - r')$, since the m_i's are pairwise co-prime.

So $r \equiv r' \pmod{(\Pi m_i)}$, and so $r = r'$ since both $r, r' \in \{0, 1, \ldots, (\Pi m_i) - 1\}$.

But the total number of sequences $r_0, \ldots, r_n$ such that (3) holds is precisely Πm_i.

Hence every such sequence must be a sequence of remainders of some r, $0 \le r < \Pi m_i$.

Exercise The proof of CRT just given is non-constructive. Show how to obtain efficiently the r that meets the requirement of the theorem, i.e., in polytime in n—so in particular not using brute force search.

Given two groups $(G_1, *_1)$ and $(G_2, *_2)$, a mapping $h : G_1 \longrightarrow G_2$ is a *homomorphism* if it respects the operation of the groups; formally, for all $g_1, g_1' \in G_1$, $h(g_1 *_1 g_1') = h(g_1) *_2 h(g_1')$.

If the homomorphism h is also a bijection, then it is called an *isomorphism*.

If there exists an isomorphism between two groups G_1 and G_2, we call them *isomorphic*, and write $G_1 \cong G_2$.

If $(G_1, *_1)$ and $(G_2, *_2)$ are two groups, then their product, denoted $(G_1 \times G_2, *)$ is simply $\{(g_1, g_2) : g_1 \in G_1, g_2 \in G_2\}$, where $(g_1, g_2) * (g_1', g_2')$ is $(g_1 *_1 g_1', g_2 *_2 g_2')$.

The product of n groups, $G_1 \times G_2 \times \cdots \times G_n$ can be defined analogously; using this notation, the CRT can be stated in the language of group theory as follows:

If $m_0, m_1, \ldots, m_n$ are pairwise co-prime integers, then $\mathbb{Z}_{m_0 \cdot m_1 \cdot \ldots \cdot m_n} \cong \mathbb{Z}_{m_0} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$.