Review Notes: The General Case

Spencer Martz

May 1, 2024

1 Modular arithemtic and applications to key codes

1.1 The order of an integer mod n

Definition Let $n \geq 1$, then $a \in \mathbb{Z}$ is said to have finite multiplicitive order (fmo) if

$$\exists k \in \mathbb{P} \; s.t. \; [a]_n^k = [1]_n \tag{1}$$

In that case, the order of a (mod n) is said to be the least integer k that has this property.

Theorem 1.6.1

The integer a has fmo if and only if a is coprime to n.

Proof For the forward, suppose a has finite order mod n, then we have $a^k \equiv 1 \mod n$, thus $a^{k-1}a \equiv 1 \mod n$, and so $[a]_n$ has an inverse ($[a]_n^{k-1}$), which implies (a,n)=1 by theorem 1.4.3.

Now the converse, suppose (a,n) =1. Again by theorem 1.4.3 a has an inverse, and so is in G_n (the set of invertible congruence classes). By theorem 1.4.7, any product of elements in G_n is also in G_n, so it follows any $[a]^k$ is invertible. Consider the powers of [a] upto n+1:

$$[a]^1, [a]^2, [a]^3, \ldots [a]^{n+1} \tag{2}$$

Now, since there are only n distinct elements in Z_n, atleast one of these must be equal (Pidegon hole principle). Let them be $[a]^t = [a]^k$, with $1 \leq k < t \leq n+1$, so that $t - k \geq 1$ we may take:

$$\begin{aligned} [a]^t &= [a]^k \\ [a]^t - [a]^k &= 0 \\ [a]^k([a]^{t-k} - 1) &= 0 \\ [a]^{-k}[a]^k([a]^{t-k} - 1) &= 0 \\ ([a]^{t-k} - 1) &= 0 \\ [a]^{t-k} &= 1 \end{aligned}$$

So a has a finite multiplicitve order (of t-k) mod n. Note this is not neccesairly THE order of a.

Theorem 1.6.2

Suppose a has an order k mod n. Then,

$$a^r \equiv a^s \mod n \iff r \equiv s \mod k \tag{3}$$

Proof The converse is trivial: if $r \equiv s \mod k$, then we may write r=s+kt, and so

$$[a]^r = [a]^{s+kt} = [a]^s[a]^{kt} = [a]^s \qquad \text{note k is the order of a, } [a]^k = [1] \tag{4}$$

Now assume $a^r \equiv a^s \mod n$, and let $r \leq s$. Since a has an order k mod n, (a finite order), by 1.6.1 it is invertible, and again by 1.4.7 any a^r is invertible. Then we have:

$$1 \equiv [a]^{s-r} \mod n \tag{5}$$

Now, by euclidean division /theorem 1.1.1, write $s - r = qk + u$ with $0 \leq u < k$. Again since k is the order of a, we may take

$$1 \equiv [a]^{s-r} \equiv [a]^{qk+u} = [a]^u \mod n \tag{6}$$

, so u is a finite multiplicitive order of a. But $1 \leq u < k$ contradicts the minality of k, so r must be 0, and thus s-r=qk, or $r \equiv s \mod k$.

1.2 Fermat's Theorem 1.6.3

Let p be prime, and $a > 1$ *st* $p \nmid a$ (so a is coprime to p). Then

$$a^{p-1} \equiv 1 \mod p \tag{7}$$

Additionally it follows that for any a, (which could have $p|a$), $a^p \equiv a \mod p$

proof: Let G_p be the set of invertible congruence classes mod p. By 1.4.6 then, $Z_n \backslash 0 = G_n$, that is every congruence class is invertible (since they are all coprime to p), e.g.

$$G_p = \{[1], [2], [3], \ldots, [p-1]\} \tag{8}$$

Now denote by aG_p the set of a multipled with each element of G_p, that is:

$$aG_p = \{[a][b] | b \in G_p\} \tag{9}$$

Now by theroem 1.4.7, each element of aG_p is in G_p. Additionally, we cannot have some distinct b and c where $[a][b] = [a][c]$, since it directly follows that $[b] = [c]$. Therfore it is the case that $aG_p = G_p$. Now let N be the product of all elements of G_p, $[1][2][3][4][5][6] \ldots [p-1]$. Since $aG_p = G_p$, the product of their elemets is also equal. So we may write:

$$[N] = [1][2][3][4][5][6] \ldots [p-1] = [a][1][a][2][a][3][a][4][a][5][a][6] \ldots [a][p-1]. \tag{10}$$

Regrouping the right hand side gives:

$$[N] = [a]^{p-1}[1][2][3] \ldots [p-1] = [a]^{p-1}[N] \tag{11}$$

Now since [N] is invertible, we have=

$$[N]^{-1}[N] = [a]^{p-1}[N][N]^{-1} \tag{12}$$

$$1 = [a]^{p-1} \tag{13}$$

So the first result follows. Additionally, if $a|p$, $a \equiv a^r \equiv 0 \mod p$, and by the above the second result holds for all integers.

Corollary 1.6.4

Let p be a prime number, and a any number not divisble by p. Then the order of a mod p divides p-1.

Proof: Follows directly from fermat's theorem and 1.6.2

Now we define the euler phi (or totient) function, $\phi(n)$, which is the number of elements in G_n, equivalently:

1. the number of invertible congruence classes mod n,
2. the number of positive integers less then n and coprime to n

Theorem 1.6.5

For p prime, $\phi(p^n) = p^n - p^{n-1}$

Proof: First note the result clearly holds for p^1, and also note the only divisors of p^n are $p, p^2, p^3 \dots p^n$.

For p^2, we count all the numbers up to p^2 which are coprime to p^2. that is they do not do not share a factor with p^2. The only factor of p^2 is p, and so the only numbers which share a factor with p^2, are multiples of p, that is $p, 2p, \dots (p-1)p$.

So to count the numbers upto p^2 which do not share a factor, we simple remove the ones that do, multiples of p upto p^2. There are p such number, and so the total number of numbers coprime to p^2 is $p^2 - p$.

Similarly, for p^k, we must remove the $p^k - 1$ multiples of p less then p^k : $\{ap | 1 \leq a \leq p^k - 1\}$ (noting $p^{k-1}p = p^k$). Thus the number of integers coprime to p^k is $p^k - p^{k-1}$.

Theorem 1.6.6

For a,b coprime, $\phi(ab) = \phi(a)\phi(b)$. Proof: Let $[r]_a$ and $[s]_b$ be elements of G_a, G_b respectively. Now, my the chinese remainder theorem, there is an integer t satifying:

$$t \equiv r \mod a \tag{14}$$
$$t \equiv s \mod b \tag{15}$$
$$\tag{16}$$

which is unique upto congruence mod ab. Additionally, this $[t]_{ab}$ is invertible, since by the above we have that r=t+ka for some integer k, and since a and r are coprime, by 1.1.4 , it follows that (t,a)=1. Similarly (t,b)=1. Thus, by properties of coprime we may assume (ab,t)=1, and so $[t]_{ab}$ is invertible.

Now we show that any invertible $[t]_{ab}$ is the product of some unqiue $[r]_a$ and $[s]_b$, and it will follow that $|G_{ab}| = |G_a \times G_b|$ have the same number of elements. For such a $[t]_{ab}$, let r be the standard representative of $[t]_a$. Since (t,ab)=1 (and a and b are coprime), we have (t,a)=1. and, since t =ka+ r, again by 1.1.4 we have that (a,r)=1, thus $[r]_a \in G_a$. Similarly, with s being

the standard rep of $[t]_b, [s]_b \in G_b$. Thus each $[t]_a b$ determines a pair

$$t \equiv r \mod a \tag{17}$$
$$t \equiv s \mod b \tag{18}$$
$$\tag{19}$$

, and since any such $[t]_{ab}$ is unique mod ab, is follows that each pair is unqiue. Additionally, since any $r \in G_a$ is compime to any other $s \in G_b$, every element in $G_a \times G_b$ has a valid $[t]_a b$. Thus we may construct a bijection from G_{ab} to $G_a \times G_b$, and they have the same size–the result follows by definition of ϕ and noting $|X \times Y| = |X||Y|$.

Euler's Theorem 1.6.7

Euler's theorem is a generalization of Fermat's theorem to non-prime modular bases. The proof is highly similar. It states, for a coprime to n,

$$a^{\phi(n)} \equiv 1 \mod n \tag{20}$$

Proof: Let G_n and aG_n be defined as before. Then similarly, by 1.4.7, $aG_n \subset G_n$, and additionally any $[a][b] \in aG_n$ is unique, since for any $[a][b] = [a][c]$ we immediately have $[b] = [c]$.. Thus $aG_n = G_n$, and so the product of all their elements [N] is equal (and invertible). As before we may group the product aG_n to obtain

$$[N] = [a]^{\phi(n)}[N] \tag{21}$$

and since n is invertible, we have

$$[a]^{\phi(n)} = 1, \text{ or } a^{\phi(n)} \equiv 1 \mod n. \tag{22}$$

Theorem 1.6.8

Let (a,n)=1, then the order of A mod n divides d.

Proof Follows with the same reasoning from 1.6.4 (and so by 1.6.2)

1.3 Public key codes

Eulers theorem presents a method to encrypt messages which are sent publicly. To begin, the reciever constructs a code. They take two very large primes, p and q, and let

$$n = pq, \text{ The "base"} \tag{23}$$

Note then by 1.6.5 and 1.5.6, $\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)$. Then we may find some integer a (the "lock" which is coprime to $\phi(n)$, and express it with bezout's identity:

$$xa + y\phi(n) = 1 \tag{24}$$

, and note that x, (the "key") is then the inverse of $[a]_\phi(n)$.

Now the reciever publishes the base and lock, that is a and n, but keeps all other numbers secret,

To encode a message, the sender first creates a numerical representation of the message B (using ASCII for example), which are decomposed into messages B_i with strictly fewer digits then p and q. Then, using the "lock" the sender calculates the standard representative of $B_i^a \equiv m_i \mod n$. The m_i are the encryted blocks, and the sender sends these.

To decrept the message, the reciever uses the "key" x to simply calclutes the standard representative of $m^x \mod n$, since

$$m \equiv B^a \mod n \tag{25}$$

$$m^x \equiv (B^a)^x \equiv B^{ax} \equiv B^{1-y\phi(n)} = B(B^{\phi(n)})^{-y} \equiv B(1)^{-y} \equiv B \mod n. \tag{26}$$

This method is effective becuase it is simple to use, but exceedingly difficult to cract, since that would involve the highly difficult task computing large prime decompositions (or equivalently, $\phi(n)$. Since the "key" x is constructed from the gcd of a and $\phi(n)$, to compute the "key" x, a cracker must determine these two primes p and q (to determine $\phi(n)$). There is no know way to do this more efficiently then just a simple comparison search (upto sqrt(n)), which has a time complexity $O(2^{\sqrt{n}})$.

2 Permutations

Defintion Let X be any set. A partition on X, denoted $\pi(X)$, is a bijection from X to itself. For any finite set we may construct a bijection from X to $\mathbb{N}$, so the latter is used for calculations.There are two ways of representing a permutation, two-row, or cycle notation.

Theorem 4.1.1: Partitions are a group under composition

Let $n \geq 0$, and S(n) be the set of all perutations on a set with n elements. Then S(n) satifies the follows:

1. Closure: $\forall \pi, \sigma \in S(n), \pi\sigma \in S(n)$
2. Identity: $\exists id \in S(n) s.t. \forall \pi,\ id\pi = \pi id = \pi$
3. Inverse: $\forall \pi \in S(n), \exists \pi^{-1}\ s.t.\ \pi\pi^{-1} = \pi^{-1}\pi = id$

Proof: Since permutations are a bijection, we may state this as follows:

1. Closure: Any composition of bijections is a bijection.
2. Identity: The identity function is a bijection
3. Inverse: All bijections have an inverse.

All of these are proved in 2.2.4 (and trivial except for the first). Additionally we note here that S(n) has n! elements, since you have n choices for the first element, then n-1, n-2, and so on.

2.1 Disjoint permuations

Defintion: Let $Mov(\pi)$ be the elements not fixed by π, that is $\{x \in X | \pi(x) \neq x\}$. Two permutations π and σ are said to be disjoint if $Mov(pi) \cap Mov(\sigma) = \emptyset$

Theorem 4.1.2

If π and σ are disjoint, they commute–that is, $\pi\sigma = \sigma\pi$.

proof: Since π and σ are disjoint, $Mov(pi) \cap Mov(\sigma) = \emptyset$ by def. Therefore for some $m \in X$, there are three cases:

1. $m \in Mov(\pi)$
2. $m \in Mov(\sigma)$
3. $m \notin Mov(\pi) \cup Mov(\sigma)$

In all three cases, $\pi(\sigma(m)) = \sigma(\pi(m))$ (since if its moved by one, it is fixed by the other), and so it follows that $\pi\sigma = \sigma\pi$

Theorem 4.1.3

Every cycle is a product of disjoint permutations

2.2 Order and sign of a permutation

Defintion: Powers of π and Order

Theorem 4.2.1

Exponent properties: Let π be a permutation, and r,s be integers.

1. $\pi^r \pi^s = \pi^{r+s}$
2. $(\pi^r)^s = \pi^r s$
3. $\pi^{-r} = (\pi^r)^{-1}$
4. If $\pi\sigma = \sigma\pi$, then $(\pi\sigma)^r = \pi^r \sigma^r$

The first three are trivially proved by induction, (for no.3 note $(fg)^{-1} = g^{-1}f^{-1}$ for bijections. Now for no. 4, we need an addtional inductive assumption which is used in the proof, that is that $\sigma\pi^r = \pi^r\sigma$. Both hold for r=1. Now suppose inductively $(\pi\sigma)^r = \pi^r\sigma^r$ (and $\sigma\pi^r = \pi^r\sigma$). We have:

$$(\pi\sigma)^{r+1} = \pi\sigma(\pi\sigma)^r = \pi(\sigma\pi^r)\sigma^r = \pi^{r+1}\sigma r + 1 \tag{27}$$

$$\sigma\pi^{r+1} = \sigma\pi\pi^r = \pi\sigma\pi^r = \pi\pi^r\sigma = \pi^{r+1}\sigma \tag{28}$$

So by the inductive hypothesis the result holds.

Theorem 4.2.2

(perumatations have finite order) Let π be a permuation in S(n). Then there exists a positive integer k such that $\pi^k = id$.

Proof: Consider the successive powers of π, $\pi, \pi^2, \pi^3, \ldots$. Since S(n) is finite this list must repeat at some point (pidgeon hole principle). Then we may let some $\pi^r = \pi^s$ for $r > s$, and since π^s is invertible, we have $\pi^{r-s} = 1$. We say the order of π is the least positve integer m such that $\pi^m = 1$, which need not be r-s as above.

Theorem 4.2.3

Let n be the order of π, then $\pi^r = \pi^s \iff r \equiv s \mod n$.

Proof: Assume $r > s$, $\pi^r = \pi^s$, we have $\pi^{r-s} = 1$, and the converse is true as well. Thus, if we show that

$$\pi^k = id = \pi^0 \text{ (e.g. } k = s - r) \iff k \equiv 0 \mod n (k|n) \tag{29}$$

the result will follow, since we may take k=r-s for $\pi^r = \pi^s$. Now then if $n|k$, we have k=nt, thus $\pi^k = \pi^{nt} = id^t = id$.
Conversely, if $\pi^k = id$, write k in the form qn+r, for $0 \leq r < n$, and again we see that $\pi^k = id$ implies that $\pi^r = id$, which contradicts the minimality of n, thus $k = qn, k|n$.

Theorem 4.2.4

the order of a cycle is it's length

Theorem 4.2.5

Product of disjoint cycles' order is the lcm of their lengths

Theorem 4.2.6

Induction on 4.2.5

Defintion: Sign of a permuation Define the polynomial Δ as the product of $\{(x_i - x_j)|i < j\}$. Additionally, define $\pi\Delta = \prod\{(x_{pi(i)} - x_{\pi(j)}|i < j\}$ The sign of pi is defined according to:

$$sgn(\pi) = \begin{cases} -1 \; if \pi\Delta = -1 \\ 1 \; if \pi\Delta = 1 \end{cases} \tag{30}$$

From the defintion it directly follows that $\pi\Delta = sgn(\pi)\Delta$

Theorem 4.2.7

sgn(pi) is well defined

Theorem 4.2.8

Let $\sigma, \pi \in S(n)$, then $sgn(\pi\sigma) = sgn(\pi)sgn(\sigma)$

Proof: The result follows from the defintion. Since $\pi\sigma\Delta = sgn(\pi\sigma)\Delta$ by def. Additionally, $\pi\sigma\Delta$ is equivalent to applying π to $\sigma\Delta$, which is equivlent to applying π to $sgn(\sigma)\Delta$ by defition, thus $\pi\sigma\Delta = sgn(\pi\sigma)\Delta = sgn(\pi)sgn(\sigma)\Delta$, and so the result follows. Note this holds even for non disjoint permutations, and any product of permutations.

Theorem 4.2.9

Properties of sgn

1. $sgn(id) = 1$
2. $sgn(\pi) = sgn(\pi^{-1}) \iff sgn(\pi\pi^{-1}) = 1$
3. $sgn(\pi\sigma\pi^{-1}) = sgn(\sigma)$
4. If τ is a transposition, $sgn(\tau) = -1$

Theorem 4.2.10

Every cycle is a product of transpositions

Proof

$$(x_1x_2x_3 \dots x_n) = (x_1x_n)(x_1x_{n-1}) \dots (x_1x_3)(x_1x_2) \quad (n - 1terms) \tag{31}$$

Theorem 4.2.11

The sign of pi occurs as the total number of transpositoins in a decomposition is even (+1) or odd (-1). Additionally, the sgn of pi is -1 if in it's unqiue cycle decomposition it has an odd number of length cycles, and is 1 if not. The first part follows since each permutation may unqiely be decompsed into it's disjoint cycles, which may then be decomponsed into transpositions $\tau_1\tau_1 \dots \tau_n$ is Then the sign of pi is -1^n, and the result follows. The second result follows, since cycles of even length decompose into products of an odd number of transpositions, or vise versa. If we only have odd length cycles, the sign is one. Each even length cycle multiples the sign by negative one (since they decompose into an odd number of transpositions).

3 Groups

Defintion of a group A group (G,*) is a set, denoted G, together with an operation, often denoted with * or simply concatenations , which obeys the following properties:

1. Closure:
2. Associativity
3. Exisitece of Identity
4. Existence of Invevrse

Theorem 4.3.1

Uniqueness of the inverse.

3.1 Examples of groups

3.1.1 Numerical groups

3.1.2 Symmetry groups

+