DIVISIBILITY AND GROUPS

SECOLINSKY

Our study begins with divisibility. We introduce first the concepts of greatest common divisor and least common multiple of two integers. Let $a, b \in \mathbb{Z}$, $D = \{d \in \mathbb{Z}_+ : d|a \wedge d|b\}$, and $M = \{m \in \mathbb{Z}_+ : a|m \wedge b|m\}$. Then d^* is the greatest common divisor of a, b means that

$$[d^* \in D \wedge \forall d \in D, d|d^*]$$

and will be denoted as (a, b). To say that m^* is the least commom multiple of a and b means that

$$[m^* \in M \wedge \forall m \in M, m^*|m]$$

and is denoted as $[a, b]$.

Our first statement about divisors will be that the product of two relatively prime divisors of a number is a divisor of that number too. Our method of proof uses the fact that (a, b) can be expressed as a linear combination of a and b.

Statement 1. *Let $c \in \mathbb{Z}$, $a, b \in \mathbb{Z}_+$, $(a, b) = 1$, and $a|c$, $b|c$. Then $ab|c$.*

Proof. Since $(a, b) = 1$, there's $h_1, h_2 \in \mathbb{Z}$ such that $1 = ah_1 + bh_2$. So $c = ach_1 + bch_2$ and because $c = bp = am$ for some $m, p \in \mathbb{Z}$, $c = a(bp)h_1 + b(am)h_2 = ab(ph_1 + mh_2)$. Thus $ab|c$. □

There is plenty to say about divisibility. So we continue with noting that the least common multiple of a and b is ab if a and b are relatively prime.

Statement 2. *Let $a, b \in \mathbb{Z}_+$. Then $(a, b) = 1 \Rightarrow [a, b] = ab$.*

Proof. First note that $ab \in M = \{m \in \mathbb{Z}_+ : a|m \wedge b|m\}$. Now let $m \in M$ so that $a|m$ and $b|m$, and since a and b are relatively prime, $ab|m$. So we have that $ab \in M$ and $ab|m$ for any multiple m of both a and b. □

The power of mathematics is the ability to generalize from what we know. For example, how would we express a more abstract Statement 2?

Statement 3. *Let $a, b \in \mathbb{Z}_+$. Then $ab = [a, b](a, b)$.*

After dividing an integer a by a positive integer n, we see that we get either a zero remainder or a positive remainder less than n. This remainder is expressed as $a \bmod n$. What follows are statements about remainders.

Statement 4. *Let $n \in \mathbb{Z}_+$ and $a, b \in \mathbb{Z}$. Then $n|a - b \Leftrightarrow a \bmod n = b \bmod n$.*

Proof. Let $a = q_1 n + r_1$ and $b = q_2 n + r_2$. So $a - b = n(q_1 - q_2) + r_1 - r_2$. If $n|a - b$, then $r_1 - r_2 = 0$ so that $a \bmod n = b \bmod n$. Conversely, If $a \bmod n = b \bmod n$, then $r_1 - r_2 = 0$ so that $n|a - b$. □

When these two integers a and b have the same remainder r upon being divided by the positive integer n, number theorists say that they belong to the same residue class $r \in \mathbb{Z}_n = \{0, \ldots, n - 1\}$.

Statement 5. *Let* $a \bmod n = r_1$ *and* $b \bmod n = r_2$. *Then* $ab \bmod n = r_1 r_2 \bmod n$ *and* $(a+b) \bmod n = (r_1 + r_2) \bmod n$.

Proof. Let $a = q_1 n + r_1$ and $b = q_2 n + r_2$. Since $n | n(q_1 + q_2) = (a+b) - (r_1 + r_2)$, $(a+b) \bmod n = (r_1 + r_2) \bmod n$. Also, because $n | (n^2 q_1 q_2 + n r_2 q_1 + n r_1 q_2 + r_1 r_2) - r_1 r_2 = ab - r_1 r_2$, $ab \bmod n = r_1 r_2 \bmod n$. □

Statement 6. *Let* $s, t \in \mathbb{Z}_+$ *be relatively prime. Then* $a \bmod st = b \bmod st \Leftrightarrow a \bmod s = b \bmod s$ *and* $a \bmod t = b \bmod t$.

Proof. We'll first assume $a \bmod st = b \bmod st$, i.e., $st | a - b$. Thus $(st)m = a - b$,i.e., $s | a - b$ and $t | a - b$. Hence $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$. Now assume $a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$ so that $s | a - b$ and $t | a - b$. Since $(s, t) = 1$, $st | a - b$, i.e., $a \bmod st = b \bmod st$. □

Now to begin with some general statements about groups. A number-theoretic group will then be introduced afterwards.

Statement 7. *Let* G *be a group. Then* G *is cyclic* $\Rightarrow$ G *is Abelian.*

Proof. Let $G = \langle a \rangle$ and $x, y \in G$ so that $x = a^k$ and $y = a^m$ for some $k, m \in \mathbb{Z}$. Hence $xy = a^k a^m = a^{k+m} = a^{m+k} = a^m a^k = yx$. Thus G is Abelian. □

The next statements uses the subgroup notation $\leq$ and the subgroup test for a subset of a group G. This test states for a nonempty $H \subset G$, and $x, y \in H$, that H is a subgroup whenever $xy^{-1} \in H$.

Statement 8. *Consider the Abelian group* $\langle G, * \rangle$ *and* $H = \{g \in G : |g| < \infty\}$. *Then* $H \leq G$.

Proof. H isn't empty since $e \in H$. Now let $t, g \in H$ where $|t| = m$, $|g| = k$ and $r = [m, k]$. To show that H is a subgroup of G, we'll show $tg^{-1} \in H$. G is Abelian, so $(tg^{-1})^r = t^r (g^{-1})^r = t^r (g^r)^{-1} = e(e)^{-1} = e$. Thus $|tg^{-1}|$ is at most r, i.e., $|tg^{-1}| < \infty$. □

The statement that if G is a group and $H = \{g \in G : |g| < \infty\}$, then H is a subroup of G is false. To see this, consider the special linear group of $n \times n$ matrices $SL_n(\mathbb{R})$ defined as the set of all $n \times n$ matrices whose entries are in $\mathbb{R}$ and whose determinant is 1. Letting $A, B \in SL_2(\mathbb{R})$ where $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$, observe that $|A| = 4, |B| = 3$ and $|AB| = \infty$. Thus we conclude that $AB \notin H$.

We are ready to continue the number-theoretic discussion using our knowledge of divisors and groups. The group of units modulo $n > 1$ is the set $U(n) = \{x \in \mathbb{Z}_n : (x, n) = 1\}$, i.e., the positive integers less than and relatively prime to n, with the multiplicative operation modulo n. The size of $U(n)$ is given from the totient function $\phi(n)$ and is expressed in closed form as

$$n \prod_{\substack{p|n \\ p \text{ is prime}}} \left(1 - \frac{1}{p}\right).$$

Do you find it amazing that such a formula will always yield an integer? It is a fact from the theory of cyclic groups that any element of $U(n)$ is a generator of the cyclic group $\mathbb{Z}_n$ where the operation is addition modulo n. It is not always true that $U(n)$ is cyclic.

The next statement is about enumerating the elements of a finite cyclic group with a particular order d.

Statement 9. *Let G be a cyclic group of order n and $d|n$. Then $\phi(d)$ enumerates the elements in G of order d.*

Proof. Let $\langle a\rangle \leq G$ be of order d and $k \leq d$ be a positive integer. Then $\langle a\rangle = \langle a^k\rangle$ if and only if $1 = (1,d) = (k,d)$, which is when k is relatively prime to d. The result follows from $d = |\langle a\rangle| = \left|\langle a^k\rangle\right|$. □

Given an element $a \in G$ of order d, it is not always true that $a^k = a^{(k,d)}$ even though $\langle a^k\rangle = \langle a^{(k,d)}\rangle$. Take for example $U(10) = \{1,3,7,9\} = \langle 3\rangle = \langle 7\rangle$ and notice that $3^3 = 7 \neq 3 = 3^{(3,4)}$.

Now to begin establishing an identity for $U(n)$. It will be established in two ways. The first depends on algebraic manipulation of remainders. The elegance of the second approach will then be presented and will depend on one simple fact. What we are doing exemplifies the nature of mathematics: There are several ways to approach a problem.

Let $\mathbb{Z}_n^* = \{b \in \mathbb{Z}_n : (\exists x \in \mathbb{Z}_n)(1 = bx \bmod n)\}$ be equiped with the multiplication operation modulo n. This set has as elements those of $\mathbb{Z}_n$ with a multiplicative inverse modulo n. The identity of $U(n)$ is with this finite set.

Theorem 1. *$\mathbb{Z}_n^*$ is $U(n)$.*

Proof. We'll first show that $U(n) \subset \mathbb{Z}_n^*$. So let $a \in U(n)$. Since $(a,n) = 1$, let $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. So $1 = 1 \bmod n = (ax+ny) \bmod n = (ax \bmod n + ny \bmod n) \bmod n = (ax \bmod n) \bmod n = ax \bmod n = (a \bmod n)(x \bmod n) \bmod n = [a(x \bmod n)] \bmod n$. Since $1 = [a(x \bmod n) \bmod n]$, $a^{-1} = x \bmod n$. Thus $a \in \mathbb{Z}_n^*$.

Now we'll show $\mathbb{Z}_n^* \subset U(n)$. Let $x \in \mathbb{Z}_n^*$ so that $x^{-1} = b$. So $1 \bmod n = xb \bmod n$, i.e., $n|xb-1$. Then $nk = xb - 1$,i.e., $xb - nk = 1$. Now since b and k are solutions to $xu_1 - nu_2 = 1$ where u_1 ad u_2 are variables, (x,n) must divide 1 and hence $(x,n) = 1$. Thus $x \in U(n)$. □

The more elegant proof is done with one sentence: $1 = bx \bmod n$ if and only if $(b,n) = 1$. Hence b has an inverse modulo n is equivalent to b and n being relatively prime.

This $\mathbb{Z}_n^*$ is an Abelian group, and what has just been established was about two sets being equal. How about two groups? What should it mean to say that two groups are structurally the same? An alebraist's answer would be that two groups are the same structurally when they are isomorphic.

Definition(Isomorphism). *Let $< G, \circ_1 >$ and $< H, \circ_2 >$ be groups. An isomorphism is a bijective mapping $f : G \to H$ which preserves the group operation in the following sense: if $a, b \in G$, then $f(a \circ_1 b) = f(a) \circ_2 f(b)$.*

To give an example of two groups being the same in structure, an automorphism is introduced. An automorphism of a group G is an isomorphism $f : G \to G$. The set of all automorphisms is a group under function composition $\circ$ and is denoted as $Aut(G)$. It just so happens that $Aut(\mathbb{Z}_n)$ is isomorphic to $U(n)$. In symbols, we write $Aut(\mathbb{Z}_n) \cong U(n)$. There is a proof of the statement which uses the following fact.

Statement 10. *Let $r \in U(n)$ and $\alpha : \mathbb{Z}_n \to \mathbb{Z}_n$ where $\alpha(s) = sr \bmod n$. Then $\alpha \in Aut(\mathbb{Z}_n)$.*

Proof. Since $\mathbb{Z}_n = \langle r\rangle$, α is surjective. Now let $\alpha(s) = \alpha(p)$. Since $s, p \in \mathbb{Z}_n$ and $|\langle r\rangle| = n$, $s = p$. Finally, $\alpha(s+p) = (s+p)r \bmod n = (sr + pr) \bmod n = (sr \bmod n + pr \bmod n) \bmod n = \alpha(s) + \alpha(p)$. Thus $\alpha \in Aut(\mathbb{Z}_n)$. □