Divisibility

Suppose that $a, b \in \mathbb{Z}$. We say that $b$ divides $a$ exactly when there is $c \in \mathbb{Z}$ such that $a = bc$. We express the fact that $b$ divides $a$ in symbols by writing $b \mid a$.

Observations

We leave the reader to verify all of the following simple facts.

(a) $x \mid 0$ for every $x \in \mathbb{Z}$.

(b) Suppose that $y \in \mathbb{Z}$ and $0 \mid y$, then $y = 0$.

(c) Both $a \mid b$ and $b \mid a$ if and only if $|a| = |b|$.

(d) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(e) If $a \mid b$ and $k \in \mathbb{Z}$, then $a \mid kb$.

(f) If $a \mid b$ and $a \mid c$, then $a \mid (b \pm c)$.

Various relations

Suppose that $N \in \mathbb{N}$. We define a relation $\sim$ on $\mathbb{Z}$ by writing $a \sim b$ exactly when $N \mid (a - b)$. It is easy to check that $\sim$ is an equivalence relation. If $x \in \mathbb{Z}$, then the equivalence class $[x]$ which contains $x$ is $\{x + kN \mid k \in \mathbb{Z}\}$. The set of equivalence classes is written $\mathbb{Z}_N$.

An Example

Suppose that $N = 3$. There are exactly three equivalence classes of $\sim$. They are

$$\{\ldots - 9, -6, -3, 0, 3, 6, 9 \ldots\}$$

$$\{\ldots - 8, -5, -2, 1, 4, 7, 10 \ldots\}$$

and
\{ \ldots, -7, -4, -1, 2, 5, 8, 11 \ldots \}.

We could write the first of these classes as \([0], [3], [6], [-3]\), or as the equivalence class of any one of its elements. However, the square brackets can get a little annoying. We can use a bold font instead, so the first equivalence class is

\[0 = 3 - 6 = -3 = \ldots\]

If you are making hand written notes, a neat way to indicate bold type is to underline the symbol. Thus you can write \([1] = 1 = \underline{1}\).

**Addition on \(\mathbb{Z}_N\).**

Notice that \(\mathbb{Z}_N\) is a set of size \(N\), and that its distinct elements are precisely \(0, 1, \ldots, N - 1\). We want to define addition of elements of \(\mathbb{Z}_N\). We do it like this. Suppose \(x, y \in \mathbb{Z}_N\). Choose \(a \in x, b \in y\). Define \(x + y\) to be \([a + b]\). Notice that the plus sign in \([a + b]\) indicates addition of integers.

Now, there is something rather dodgy about this recipe. To illustrate the problem, we make a diversion. Let \(P\) be the set of all prime numbers, let \(C\) be the set of composite numbers and let \(U = \{1\}\). Thus the sets \(P, C, U\) are pairwise disjoint, and \(\mathbb{N} = U \cup P \cup C\). Let \(X = \{U, P, C\}\). Try to define addition on \(X\) as follows: when \(A, B \in X\), choose \(a \in A, b \in B\) and let \(A + B\) to be that element of \(X\) which contains \(a + b\).

Right, it is bright and early on Monday morning. The phone rings: someone needs to know \(P + C\) urgently. You choose \(7 \in P\) and \(6 \in C\). Now \(7 + 6 = 13 \in P\), so you answer that \(P + C = P\). The next day, the same clown phones again, claiming to have mislaid \(P + C\) and asking for it again. You choose \(3 \in P\) and \(9 \in C\). Now \(3 + 9 = 12 \in C\) so you confidently answer that \(P + C = C\). On Wednesday the punter phones once more, having found the scrap of paper on which Monday’s answer had been written. The customer is very angry. How come \(P + C\) is \(P\) on Mondays but \(C\) on Tuesdays, even though \(P \neq C\)?

The problem is that you have freedom of action; you can choose \(a \in P\) and \(b \in C\) and the set where \(a + b\) lives depends on which particular \(a\) and \(b\) you happen to select. Now, this is disturbing because we have allowed this freedom of action when trying to define addition in \(\mathbb{Z}_N\). However, in that case there is not a problem. To see this, recall that we tried to add \(x, y \in \mathbb{Z}_N\) by selecting \(a \in x, b \in y\), and declaring \(x + y\) to be \([a + b]\). Suppose we do it again (it is now Tuesday!). Choose \(\widehat{a} \in x, b \in y\). Now \(a \sim \widehat{a}\) and \(b \sim b\). Thus \(a - \widehat{a} = kN\) for some \(k \in \mathbb{Z}\) and \(b - b = lN\) for some \(l \in \mathbb{Z}\). Thus \((a + b) - (\widehat{a} + \widehat{b}) = (k + l)N\), and so \((a + b) \sim (\widehat{a} + \widehat{b})\). We conclude that \([a + b] = [\widehat{a} + \widehat{b}]\) and all is well!

We say that the addition on \(\mathbb{Z}_N\) is **well-defined**.

**Multiplication on \(\mathbb{Z}_N\).**

We define an operation \(\times\) on \(\mathbb{Z}_N\) using the obvious recipe. If \(x, y \in \mathbb{Z}_N\) we select \(a \in x, b \in y\), and declare \(x \times y\) to be \([a \times b]\). However, we are now worldly.
wise, and our doubts are definitely in place. We must check that this makes sense. Choose $\hat{a} \in x, \hat{b} \in y$. Now, $a \sim \hat{a}$ and $b \sim \hat{b}$ so $a - \hat{a} = kN$ for some $k \in \mathbb{Z}$ and $b - \hat{b} = lN$ for some $l \in \mathbb{Z}$. Thus

$$a \times b = (\hat{a} + kN) \times (\hat{b} + lN) = \hat{a} \times \hat{b} + (k + l + kl)N.$$ 

Therefore $(a \times b) \sim (\hat{a} \times \hat{b})$ and so $[a \times b] = [\hat{a} \times \hat{b}]$.

**Laws of algebra of $\mathbb{Z}_N$**

The following laws can all be directly verified using the definitions of addition and multiplication in $\mathbb{Z}_N$. Recall that $N$ is an arbitrary, but fixed, natural number.

(a) $x + y \in \mathbb{Z}_N$ whenever $x, y \in \mathbb{Z}_N$.
(b) $(x + y) + z = x + (y + z)$ whenever $x, y, z \in \mathbb{Z}_N$.
(c) $x + 0 = 0 + x = x$ whenever $x \in \mathbb{Z}_N$.
(d) If $x = [a] \in \mathbb{Z}_N$, then $[a] + [-a] = 0$.
(e) $x + y = y + x$ whenever $x, y \in \mathbb{Z}_N$.
(f) $x \times y \in \mathbb{Z}_N$ whenever $x, y \in \mathbb{Z}_N$.
(g) $(x \times y) \times z = x \times (y \times z)$ whenever $x, y, z \in \mathbb{Z}_N$.
(h) $x \times 1 = 1 \times x = x$ whenever $x \in \mathbb{Z}_N$.
(i) $x \times y = y \times x$ whenever $x, y \in \mathbb{Z}_N$.
(j) $x \times (y + z) = (x \times y) + (x \times z)$ whenever $x, y, z \in \mathbb{Z}_N$.

Properties (a)–(d) ensure that $\mathbb{Z}_N$ is a group under addition. Property (e) ensures that this group is abelian (commutative). Properties (f)–(h) ensure that $\mathbb{Z}_N$ is a monoid under multiplication (a monoid is just like a group, except that the inverse axiom is missing). Property (i) ensures that this monoid is abelian (commutative). Property (j) is the distributive law of multiplication over addition, which is the only property we have which tells us how multiplication and addition interact.

Notice that the laws of algebra of $\mathbb{Z}_N$ are very familiar. If you replace $\mathbb{Z}_N$ by $\mathbb{Z}$ throughout the list, every single law remains valid. However, do not be deceived. Some strange mathematics can happen in $\mathbb{Z}_N$. For example, in $\mathbb{Z}_4$ we have $2 \times 2 = 0$. This seems very odd at first. The product of non-zero elements of $\mathbb{Z}_N$ can sometimes be 0. This disturbing state of affairs disappears in the case that $N$ is a prime number, and only in that case, as we will see in the next section.

We will allow ourselves to denote multiplication by juxtaposition in future.
Congruence notation

The notation \( a \sim b \) to indicate that \( N \mid (a - b) \) suffers from two drawbacks. It suppresses the rôle of \( N \), and it is not the notation in common use. The standard notation is \( a \equiv b \mod N \). Here \( \equiv \) is pronounced “is congruent to”, and “mod” is short for \textit{modulus}. The number \( N \) is called the \textit{modulus} of the congruence. Thus \( 1 \equiv 3 \mod 2 \), \(-7 \equiv 2 \mod 3 \) and \( 2^{10} \equiv 4 \mod 10 \).

All the fuss about addition and multiplication being well-defined amounts to the following. Suppose \( a, b, c, d \in \mathbb{Z} \) and \( N \in \mathbb{N} \). If \( a \equiv b \mod N \) and \( c \equiv d \mod N \), then both \( a + c \equiv b + d \mod N \) and \( ac \equiv bd \mod N \).

Now suppose that \( M \in \mathbb{N} \) is a natural number such that \( M \mid N \), it follows that if \( a \equiv b \mod N \), then \( a \equiv b \mod M \).

Greatest Common Divisors

The structure \( \mathbb{Z}/N \) is very special when \( N \) happens to be a prime number. We now develop some machinery to understand this situation. Suppose \( a, b \in \mathbb{Z} \). Let \( \Delta_{a,b} = \{d \mid d \in \mathbb{Z}, \ d \mid a, \ d \mid b\} \). Thus \( \Delta_{a,b} \) is the set of common divisors of the integers \( a \) and \( b \), so \( \Delta_{0,0} = \mathbb{Z} \). However, this is the case of least interest, so we will assume that at least one of \( a, b \) is not 0. Let \( m = \max\{|a|, |b|\} \), so \(-m \leq d \leq m \ \forall d \in \Delta_{a,b} \). The set \( \Delta_{a,b} \) is therefore finite, and is not empty because 1 \( \in \Delta_{a,b} \). Thus \( \Delta_{a,b} \) has a greatest element called the \textit{greatest common divisor} of \( a \) and \( b \). We write this divisor as \( \text{g.c.d.}(a, b) \). Notice that \( \Delta_{a,b} = \Delta_{b,a} \) so \( \text{g.c.d.}(a, b) = \text{g.c.d.}(b, a) \). Moreover \( \text{g.c.d.}(a, b) \geq 1 \) so \( \text{g.c.d.}(a, b) \in \mathbb{N} \). Thus \( \text{g.c.d.}(0, 1) = 1 \), \( \text{g.c.d.}(-4, 6) = 2 \) and \( \text{g.c.d.}(-9, -12) = 3 \).

Recall that \( p \in \mathbb{N} \) is a prime number if \( p \) has exactly two natural number divisors. Thus the first few prime numbers are

\[
2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71 \ldots
\]

Thus \( p \) is prime exactly when \( \Omega_{p,p} = \{-p, -1, 1, p\} \) has size 4. From the point of view of greatest common divisors, the important point about a prime number \( p \) is that if \( a \in \mathbb{Z} \), then \( \text{g.c.d.}(a, p) \) must be 1 or \( p \). Moreover \( \text{g.c.d.}(a, p) = 1 \) unless \( p \mid a \), in which case \( \text{g.c.d.}(a, p) = p \).

Division

\textbf{Theorem}[Remainder Theorem] Suppose that \( a, b \in \mathbb{Z} \) and \( b \neq 0 \). It follows that there are uniquely determined \( q, r \in \mathbb{Z} \) with \( 0 \leq r < |b| \) such that \( a = qb + r \).

\textbf{Proof} Let \( \Gamma_{a,b} = \{a + \mu b \mid \mu \in \mathbb{Z}\} \). The set \( \Gamma_{a,b}^+ = \Gamma_{a,b} \cap \mathbb{N} \cup \{0\} \) is not empty (in fact \( \Gamma_{a,b}^+ \) contains arbitrarily positive and negative integers). Let \( r = \min \Gamma_{a,b}^+ \) so \( r \geq 0 \) and \( a - r = qb \) for some \( q \in \mathbb{Z} \). Thus \( a = qb + r \) with \( q, r \in \mathbb{Z} \), \( 0 \leq r < |b| \).

Now suppose \( \tilde{q}, \tilde{r} \in \mathbb{Z} \), \( 0 \leq \tilde{r} < |b| \) and \( a = \tilde{q}b + \tilde{r} \). Subtracting we find that

\[
0 = a - a = (q - \tilde{q})b + (r - \tilde{r}).
\]
Thus \( b \) divides \( r - \hat{r} \) but \(-|b| < r - \hat{r} < |b|\). We conclude that \( r - \hat{r} = 0 \), so \( r = \hat{r} \). Thus \( qb = \hat{q}b \) and so \((q - \hat{q})b = 0 \). However, \( b \neq 0 \) so \( q = \hat{q} \) and we have established uniqueness.

**Divisors**

Suppose that \( a, b \in \mathbb{Z} \) are not both zero. Let

\[
\Omega_{a,b} = \{\lambda a + \mu b \mid \lambda, \mu \in \mathbb{Z}\}.
\]

The set \( \Omega_{a,b} \) contains both positive and negative integers. Let \( t \) be the least positive element of \( \Omega_{a,b} \).

**Proposition** In this notation we have:

(i) \( t \) divides both \( a \) and \( b \).

(ii) If \( d \) divides both \( a \) and \( b \), then \( d \) divides \( t \).

(iii) \( t = \gcd(a, b) \).

**Proof** \( 0 < t \in \mathbb{Z} \). Thus \( a = qt + r \) according to the Remainder Theorem, so \( r \geq 0 \). Now \( r = a - qt \in \Omega_{a,b} \) violates the minimality of \( t \) unless \( r = 0 \). Thus \( t \) divides \( a \). Similarly \( t \) divides \( b \), so \( t \) is a common divisor of \( a \) and \( b \) and (i) is established.

If \( d \) divides both \( a \) and \( b \), then \( d \) divides all elements of \( \Omega_{a,b} \) so \( d \) divides \( t \) and (ii) is established. Now (iii) follows from (i) and (ii).

**Euclid’s algorithm**

Suppose \( a, b \in \mathbb{Z} \) and \( b \neq 0 \). Let \( a_0 = a \) and \( a_1 = |b| \). Given that \( a_i \) has been defined for all \( i \leq n \), if \( a_n = 0 \) let \( d = a_{n-1} \) and stop the procedure. On the other hand, if \( a_n \neq 0 \) then apply the Remainder Theorem to find integers \( q_n, a_{n+1} \) such that \( a_{n-1} = q_n a_n + a_{n+1} \). Notice that \( a_n > a_{n+1} \) whenever \( n \geq 1 \), so the integers \( a_n \) form a decreasing sequence of non-negative integers for \( n \geq 1 \). This procedure must terminate after finitely many steps, and \( d = a_m \) is defined at stage \( m \). This procedure is called *Euclid’s Algorithm*.

Consider the various equations \( a_{n-1} = q_n a_n + a_{n+1} \) and \( a_{n-1} = a_n a_n = a_{n+1} \). From these it follows that (i) any common divisor of \( a_{n-1} \) and \( a_n \) divides \( a_{n+1} \) and moreover (ii) any common divisor of \( a_{n} \) and \( a_{n+1} \) divides \( a_{n-1} \). Thus \( \gcd(a_{n-1}, a_n) = \gcd(a_n, a_{n+1}) \) for every \( 1 \leq n \leq m \). It follows that

\[
\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_m, a_{m+1}) = \gcd(t, 0) = t.
\]
Primes and Products

**Proposition** Suppose that \( p \) is a prime number, and that \( a, b \) are integers. It follows that if \( p \mid ab \), then either \( p \mid a \) or \( p \mid b \).

**Proof** Suppose (for contradiction) that \( p \nmid a \) and \( p \nmid b \). Thus \( g.c.d.(p,a) = 1 = g.c.d.(p,b) \). Thus there are \( \lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{Z} \) such that \( 1 = \lambda_1 p + \mu_1 a \) and \( 1 = \lambda_2 p + \mu_2 b \). Multiply these equations so

\[
1 = \lambda_1 \lambda_2 p^2 + \lambda_1 \mu_2 b + \lambda_2 \mu_1 a + \mu_1 a \mu_2 b.
\]

Tidy up by putting \( \lambda = \lambda_1 \lambda_2 p + \lambda_1 \mu_2 b + \lambda_2 \mu_1 a + \mu_1 a \mu_2 b \). It follows that \( \lambda = \lambda_1 \lambda_2 p + \lambda_1 \mu_2 b + \lambda_2 \mu_1 a + \mu_1 a \mu_2 b \). We now have \( 1 = \lambda p + \mu ab \). It follows that \( p \nmid ab \). However, this is absurd, so we are done.

**Corollary 1** (i) If \( p \) is prime and \( a, b \in \mathbb{Z}_p \) are such that \( ab = 0 \), then either \( a = 0 \) or \( b = 0 \). (ii) If \( a \in \mathbb{Z}_p \) and \( a \neq 0 \), then there is \( \lambda \in \mathbb{Z}_p \) such that \( a \lambda = 1 \).

This is because if \( a = [a] \), then there are \( \lambda, \mu \in \mathbb{Z} \) such that \( \lambda a + \mu b = 1 \).

**Corollary 2** If \( a_1, a_2, \ldots, a_m \in \mathbb{Z} \) and \( p \) is a prime number with \( p \mid \prod_{i=1}^m a_i \), the \( p \mid a_i \) for some \( 1 \leq j \leq m \).

It follows from part (ii) of the first corollary that the non-zero elements of \( \mathbb{Z}_p^* \) of \( \mathbb{Z}_p \) form a group under multiplication of order \( p - 1 \). By Lagrange’s Theorem we have \( a^{p-1} = 1 \) for all \( a \in \mathbb{Z}_p \). Translated into the language of congruences we obtain that if the integer \( a \) is not divisible by the prime number \( p \), we have \( a^p \equiv a \mod p \). Allowing for the case that \( p \) divides \( a \), we have \( a^p \equiv a \mod p \) for all integers \( a \). Either of the last two results is sometimes called Fermat’s Little Theorem.

**Bonus: The Fundamental Theorem of Arithmetic**

**Theorem**[Fundamental Theorem of Arithmetic] Suppose that \( n \in \mathbb{N} \), and \( n > 1 \). It follows that \( n \) can be expressed as a product \( \prod_{i=1}^t p_i^{n_i} \) of distinct prime numbers \( p_i \) and that (up to commutativity) this factorization is unique.

**Proof** We first show, by complete induction on \( n \), that every \( n \in \mathbb{N} \) with \( n > 1 \) is the product of prime numbers. It is not strictly necessary to begin complete inductions, but let us do it for safety! The smallest natural number bigger than 1 is 2, and that is \( \prod_{i=1}^t p_i^{n_i} \) with \( t = 1, p_1 = 2 \) and \( n_1 = 1 \). Now suppose that \( m \) is an arbitrary natural number bigger than 1. Either \( m \) is prime, in which case it is its own prime factorization (as 2 was), or it is composite. In the latter case \( m = m_1 m_2 \) with \( 1 < m_1, m_2 < m \) and \( m_1, m_2 \in \mathbb{N} \). Now each of \( m_1, m_2 \) is a product of prime numbers by inductive hypothesis, so \( m \) is a product of prime numbers. By complete induction we are done.

Now for uniqueness. Again we proceed by complete induction, the base case being unnecessary or a matter of staring at 2, depending on your degree of nervousness. Suppose that \( n \in \mathbb{N} \) with \( n > 1 \) has two rival factorizations \( n = \prod_{i=1}^t p_i^{n_i} \) and \( n = \prod_{j=1}^s q_j^{m_j} \). Here the \( p_i \) are pairwise distinct primes, and the \( q_j \) are pairwise distinct primes. Now \( p_1 \mid n \) so \( p_1 \mid \prod_{j=1}^s q_j^{m_j} \). Thus \( p_1 \mid q_j \) for some \( j \) by the second corollary. Thus \( p_1 = q_j \) and \( n/p_1 = n/q_j \). This last
equation, together with induction, ensures that the induced factorizations of \( n/p_1 \) and \( n/q_j \) co-incide (up to commutativity). We are done.