CHAPTER 7

Number Theory – divisors and multiples

7.1 Greatest common divisor

Definition 7.1.1. The **greatest common divisor** (or **highest common factor**) of two integers a, b, written $\gcd(a, b)$ or $\mathrm{hcf}(a, b)$ or just (a, b) is the largest natural number that divides both a and b. For example, $(10, 16) = 2$.

Observe that, if d is any *common divisor* of a and b then $d \mid a - bm$, for any integer m. Conversely, any *common divisor* of $a-bm$ and b, where $m \in \mathbb{Z}$, is a divisor of $a = (a-bm)+mb$. So the set of common divisors of a and b is also the set of common divisors of $a - bm$ and b, for any $m \in \mathbb{Z}$. In particular, this means that $(a, b) = (a - bm, b)$ for any integer m. This fact is the central idea behind the Euclidean Algorithm (Algorithm 7.1.3).

Definition 7.1.2. The **lowest common multiple** (or **least common multiple**) of a and b, written $\mathrm{lcm}(a, b)$, is the least natural number m such that $a \mid m$ and $b \mid m$.

It can be shown that

$$\gcd(a, b)\,\mathrm{lcm}(a, b) = |ab|.$$

Below we introduce an efficient way of calculating the gcd of pairs of integers, that remains useful even when the integers are very large. The method we'll use is an old one.

The Euclidean Algorithm

Algorithm 7.1.3 (Euclidean Algorithm). *To find* $\gcd(a, b)$ *where* a *and* b *are positive integers. We'll assume that* $a \geqslant b$*. The algorithm proceeds by finding pairs of integers* (q_i, r_i) *as follows:*

$$\begin{aligned}
a &= q_1 b + r_1, && 0 \leqslant r_1 < b \\
b &= q_2 r_1 + r_2, && 0 \leqslant r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3, && 0 \leqslant r_3 < r_2 \\
&\vdots \\
r_k &= q_{k+2} r_{k+1} + r_{k+2}, && 0 \leqslant r_{k+2} < r_{k+1} \\
&\vdots
\end{aligned}$$

The algorithm continues until $r_{k+2} = 0$*, so that we finish with*

$$r_{n-1} = q_{n+1} r_n,$$

with $r_{n+1} = 0$*, for some positive integer* n*.*
We will see later that being able to trace the algorithm backwards is just as valuable as obtaining $\gcd(a, b)$. In doing so, it will be useful to assign the labels:

$$a = r_{-1}, \quad b = r_0.$$

Theorem 7.1.4. *When the Euclidean Algorithm terminates we have*

$$r_n = (a, b).$$

*The assumption $a \geqslant b$ is actually unnecessary. If $a < b$ one obtains $q_1 = 0, r_1 = a$, so that the first iteration effectively swaps a and b. Thus a computer program does not need to (and for efficiency, should not) check whether or not $a \geqslant b$.

Proof. This follows from the observation we made after Definition 7.1.1, namely that $(a, b) = (a - bm)$ for any $m \in \mathbb{Z}$. At step $k + 2$, we have

$$r_{k+2} = r_k - q_{k+2}r_{k+1},$$

so that we have

$$\begin{aligned}(a, b) = (r_{-1}, r_0) &= (r_1, r_0) = (r_0, r_1)\\ &= (r_1, r_2)\\ &\vdots\\ &= (r_k, r_{k+1})\\ &\vdots\\ &= (r_{n-1}, r_n)\\ &= (r_n, r_{n+1}) = (r_n, 0) = r_n.\end{aligned}$$

Hence the last non-zero remainder r_n, of the Euclidean Algorithm, is (a, b), as claimed. □

Example 7.1.5. *Find the greatest common divisor of 1547 and 560.*
We set $a = 1547, b = 560$. Then

$$\begin{aligned}1547 &= 2 \times 560 + 427\\ 560 &= 1 \times 427 + 133\\ 427 &= 3 \times 133 + 28\\ 133 &= 4 \times 28 + 21\\ 28 &= 1 \times 21 + 7\\ 21 &= 3 \times 7 + 0\end{aligned}$$

So $(1547, 560) = 7$.

A convenient way to execute the algorithm that helps one keep track of things is via a **division table**. We demonstrate this technique below, redoing the above example:

	1547	560	
2	1120	427	1
	427	133	
3	399	112	4
	28	21	
1	21	21	3
	7	0	

Remark 7.1.6. Observe that for each i we have $r_{i+2} < r_i$. So the algorithm finishes fairly quickly.

Theorem 7.1.7 (Bézout's Lemma). *If $(a, b) = d$ then there exist integers x and y such that*

$$d = xa + yb.$$

Proof. Tracing the Euclidean Algorithm backwards, we have that r_n is a linear combination of r_{n-1} and r_{n-2}:

$$r_n = r_{n-2} - q_n r_{n-1}.$$

Substituting for r_{n-1}, using the previous step of the Euclidean Algorithm, one has r_n as a linear combination of r_{n-2} and r_{n-3}. Continuing in this way, one eventually has r_n as a linear combination of $r_{-1} = a$ and $r_0 = b$. (See the final remark of the description of Algorithm 7.1.3.)

We demonstrate the procedure, using the pair $a = 1547, b = 560$ from the previous example:

$$\begin{aligned}
7 &= 28 - 1 \times 21 \\
&= 28 - 1(133 - 4 \times 28) \\
&= 5 \times 28 - 133 \\
&= 5 \times (427 - 3 \times 133) - 133 \\
&= 5 \times 427 - 16 \times 133 \\
&= 5 \times 427 - 16 \times (560 - 427) \\
&= 21 \times 427 - 16 \times 560 \\
&= 21 \times (1547 - 2 \times 560) - 16 \times 560 \\
&= 21 \times 1547 - 58 \times 560.
\end{aligned}$$

So $(1547, 560) = 1547x + 560y$ with $x = 21$ and $y = -58$. □

Remark 7.1.8. In Theorem 7.1.7, the pair of integers (x, y) is not unique, for suppose (x_0, y_0) satisfies

$$d = ax + by, \tag{7.1.1}$$

then

$$\begin{aligned}
d &= ax_0 + by_0 \\
&= ax_0 + \lambda ab/d + by_0 - \lambda ab/d \\
&= a(x_0 + \lambda b/d) + b(y_0 - \lambda a/d).
\end{aligned}$$

Hence

$$x = x_0 + \lambda b/d, \quad y = y_0 - \lambda a/d, \tag{7.1.2}$$

where $\lambda \in \mathbb{Z}$, is a more general solution of (7.1.1). In fact, when $d = (a, b)$ one can show (7.1.2) is the most general solution of (7.1.1).

Definition 7.1.9. An equation of form

$$ax + by = c, \tag{7.1.3}$$

where x, y are unknown integers is a **linear Diophantine equation**.
Exercise. Show that (7.1.3) has solutions if and only if $\gcd(a, b) \mid c$.

Definition 7.1.10. If $(a, b) = 1$ then a and b are **relatively prime** (or **coprime**).

Corollary 7.1.11. *Integers a and b are relatively prime if and only if $\exists x, y \in \mathbb{Z}$ such that*

$$ax + by = 1.$$

Proof. The "only if" part is immediate from Theorem 7.1.7. In the other direction, suppose that $(a, b) = d$ and for a contradiction suppose that $d > 1$. Then since $d \mid ax + by$ we cannot have $ax + by = 1 \not\downarrow$, and hence, in fact $d = 1$. □

Extended Euclidean Algorithm

By reorganising our **division table**, and doing a few extra calculations on the forward trace of the Euclidean Algorithm, we can obtain coefficients x, y such that $d = (a, b)$ and

$$ax + by = d.$$

The table is organised with the following column headings:

i	x_i	y_i	r_i	q_i

Defining $a = r_{-1}$, $b = r_0$ and q_i and r_i as before, so that we have

$$r_i = r_{i-2} - q_i r_{i-1}, \text{ for } i \geqslant 1,$$

we define the x_i and y_i to satisfy the same relation as r_i, i.e.

$$x_i = x_{i-2} - q_i x_{i-1}$$
$$y_i = y_{i-2} - q_i y_{i-1}$$

for $i \geqslant 1$. As with the r_i, in order to be able to start, we must define x_{-1}, x_0, y_{-1}, y_0. We define these in such a way (and we show this below) that

$$ax_i + by_i = r_i, \text{ for } -1 \leqslant i \leqslant n,$$

so that when $i = n$ we have

$$ax_n + by_n = r_n = d,$$

i.e. the final line of the table has coefficients $x = x_n$, $y = y_n$ satisfying

$$ax + by = d.$$

Magic! The starting values for x_i and y_i are

$$x_{-1} = 1, \quad x_0 = 0, \quad y_{-1} = 0, \quad y_0 = 1.$$

One can sometimes save a step by allowing *negative* remainders. Before proving the algorithm works, let us demonstrate using our earlier example:

i	x_i	y_i	r_i	q_i	Comments
-1	1	0	1547		
0	0	1	560		
1	1	-2	427	2	$1547 - 2 \cdot 560 = 427$, $1 - 2 \cdot 0 = 1$, $0 - 2 \cdot 1 = -2$
2	-1	3	133	1	$560 - 1 \cdot 427 = 133$, $0 - 1 \cdot 1 = -1$, $1 - 1 \cdot -2 = 3$
3	4	-11	28	3	$427 - 3 \cdot 133 = 28$, $1 - 3 \cdot -1 = 4$, $-2 - 3 \cdot 3 = -11$
4	-21	58	-7	5	$133 - 5 \cdot 28 = -7$, $-1 - 5 \cdot 4 = -21$, $3 - 5 \cdot -11 = 58$

Observe that we may stop since $-7 \mid 28$. Thus from the last line of the table we have

$$-21 \cdot 1547 + 58 \cdot 560 = -7$$
$$\therefore 21 \cdot 1547 - 58 \cdot 560 = 7.$$

Proof (of Extended Euclidean Algorithm). We need to prove the claim that

$$ax_i + by_i = r_i, \text{ for } -1 \leqslant i \leqslant n,$$

given that each of x_i, y_i, r_i satisfy the recurrence

$$u_i = u_{i-2} - q_i u_{i-1}, \text{ for } i \geqslant 1,$$

and for $i = -1, 0$,

$$x_{-1} = 1, \quad x_0 = 0, \quad y_{-1} = 0, \quad y_0 = 1, \quad r_{-1} = a, \quad r_0 = b.$$

Thus, define

$$P(i) : r_i = ax_i + by_i.$$

We will prove $P(i)$ for $-1 \leqslant i \leqslant n$ by a (finite) induction by proving each of $P(-1)$, $P(0)$, and $P(k)$ and $P(k+1) \implies P(k+2)$ for general k.

For $P(-1)$, we have

$$\begin{aligned} \text{LHS of } P(-1) = r_{-1} &= a \\ &= a \cdot 1 + b \cdot 0 \\ &= a \cdot x_{-1} + b \cdot y_{-1} = \text{RHS of } P(-1) \end{aligned}$$

So $P(-1)$ holds.

For $P(0)$, we have

$$\begin{aligned} \text{LHS of } P(0) = r_0 &= b \\ &= a \cdot 0 + b \cdot 1 \\ &= a \cdot x_0 + b \cdot y_0 = \text{RHS of } P(0) \end{aligned}$$

So $P(0)$ holds.

Now we show $P(k)$ and $P(k+1) \implies P(k+2)$, for general k.
So assume $P(k)$ and $P(k+1)$, i.e.

$$\begin{aligned} r_k &= ax_k + by_k \\ r_{k+1} &= ax_{k+1} + by_{k+1} \end{aligned}$$

and consider $P(k+2)$:

$$\begin{aligned} \text{LHS of } P(k+2) &= r_{k+2} \\ &= r_k - q_{k+2} r_{k+1}, && \text{by the given recurrence} \\ &= ax_k + by_k - q_{k+2}(ax_{k+1} + by_{k+1}), && \text{by the inductive assumption} \\ &= a(x_k - q_{k+2}x_{k+1}) + b(y_k - q_{k+2}y_{k+1}) \\ &= ax_{k+2} + by_{k+2}, && \text{by the given recurrence} \\ &= \text{RHS of } P(k+2) \end{aligned}$$

So we have shown that $P(k)$ and $P(k+1) \implies P(k+2)$.

So the induction is complete and the claim

$$ax_i + by_i = r_i, \text{ for } -1 \leqslant i \leqslant n,$$

is proved. □

7.2 Congruence modulo m

Definition 7.2.1. Let $m \in \mathbb{N}$. Then we say,

$$\begin{aligned} & a \text{ is } \textbf{congruent} \text{ to } b \textbf{ modulo } m \\ \text{written: } & a \equiv b \pmod{m} \\ \iff & m \,|\, a - b \\ \iff & a - b = qm \text{ for some integer } q \\ \iff & a = b + qm \text{ for some integer } q \\ \iff & a = b + \text{“some multiple of } m\text{”}. \end{aligned}$$

Properties 7.2.2 (Properties of Congruence modulo m).

(i) $a \equiv a \pmod{m}$ *for all* $a \in \mathbb{Z}$ ***(reflexivity)***

(ii) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$ ***(symmetry)***

(iii) $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$ ***(transitivity)***

(iv) If

$$\begin{aligned} a &\equiv b \pmod{m} \text{ and} \\ c &\equiv d \pmod{m} \end{aligned}$$

then

$$\begin{aligned} (1) \qquad a + c &\equiv b + d \pmod{m}, \\ (2) \qquad ac &\equiv bd \pmod{m}, \\ (3) \qquad a^n &\equiv b^n \pmod{m} \text{ for all } n \in \mathbb{N}. \end{aligned}$$

Proof. Properties (i)–(iii) prove *congruence modulo* m is an equivalence relation on $\mathbb{Z}$.
(i) holds, since $m \,|\, 0 = a - a$.
(ii) holds, since $m \,|\, (a - b) \implies m \,|\, (b - a)$.
(iii) holds, since $m \,|\, (a - b)$ and $m \,|\, (b - c) \implies m \,|\, (a - c) = (a - b) + (b - c)$.
Now, for the parts of (iv), assume $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then for some $k, \ell \in \mathbb{Z}$,

$$a = b + km \qquad (\S)$$
$$c = d + \ell m \qquad (\dagger)$$

So,

$$\begin{aligned} (\S) + (\dagger) : a + c &= b + d + (k + \ell)m \\ &\equiv b + d \pmod{m} \end{aligned}$$

Hence, (1) holds. Also,

$$\begin{aligned} (\S) \cdot (\dagger) : ac &= (b + km)(d + \ell m) \\ &= bd + (kd + b\ell + k\ell m)m \\ &\equiv bd \pmod{m} \end{aligned}$$

So, (2) holds.
Finally, (3) follows from (2) by induction. □

Definition 7.2.3. If $a \in \mathbb{Z}$ and $m \in \mathbb{N}$, the binary operations **div** and **mod** are defined to return the *quotient* and *remainder* when a is divided by m according to the *Division Algorithm*, i.e. if $q, r \in \mathbb{Z}$ with $0 \leqslant r < m$ and

$$a = mq + r,$$

then

$$\begin{aligned} a \operatorname{div} m &= q, \text{ and} \\ a \bmod m &= r. \end{aligned}$$

Essentially, div does "integer division" of a by m. (Sometimes **quo** is used in place of div.) Most computing languages define some sort of mod operation, extended to allow negative m. The key property of interest to us, is that,

If $a \bmod m = r$ then $a \equiv r \pmod{m}$.

Note 7.2.4. Divisibility statements can be written in terms of congruences. In particular,

$$\begin{aligned} b \vdots m &\iff m \,|\, b \\ &\iff b \equiv 0 \pmod{m}. \end{aligned}$$

Notation 7.2.5. Suppose $N \in \mathbb{N}$ has decimal digit expansion

$$N = 10^n a_n + 10^{n-1} a_{n-1} + \cdots + 10a_1 + a_0 = \sum_{k=0}^{n} 10^k a_k,$$

where $a_k \in \{0, 1, \ldots, 9\}$ for $0 \leqslant k \leqslant n$. Then:

(i) $N = \overline{a_n a_{n-1} \ldots a_1 a_0}$ is called the **decimal representation** of N;

(ii) $S(N) = \sum_{k=0}^{n} a_k$ is the **sum of digits of** N; and

(iii) $A(N) = \sum_{k=0}^{n} (-1)^k a_k$ is the **alternating sum of digits of** N.

Lemma 7.2.6. *$N \equiv S(N) \pmod{m}$ where $m \in \{3, 9\}$.*

Proof. Let $\overline{a_n a_{n-1} \ldots a_1 a_0}$ be the decimal representation of N, and observe that 10 is congruent to 1 modulo each of 3 or 9. Then

$$\begin{aligned} N &= \overline{a_n a_{n-1} \ldots a_1 a_0} \\ &= \sum_{k=0}^{n} 10^k a_k \\ &\equiv \sum_{k=0}^{n} 1^k a_k \pmod{3} \\ &\equiv \sum_{k=0}^{n} a_k \pmod{3}. \end{aligned}$$

But $\sum_{k=0}^{n} a_k = S(N)$. The argument is identical if '(mod 3)' is replaced by '(mod 9)'. □

Corollary 7.2.7. *(i)* $3 \,|\, N \iff 3 \,|\, S(N)$. *(ii)* $9 \,|\, N \iff 9 \,|\, S(N)$.

Proof. This is the special case of Lemma 7.2.6 when $N \equiv 0 \pmod{m}$, for each value of m, written in terms of divisibility. □

Lemma 7.2.8. $N \equiv A(N) \pmod{11}$.

Corollary 7.2.9. $11 \,|\, N \iff 11 \,|\, A(N)$.

Remark 7.2.10. One usually describes $A(N)$ as the '*difference of the sums of even-place and odd-place digits*'. Lemma 7.2.8 is proved by observing that $10 \equiv -1 \pmod{11}$, deducing $N \equiv A(N) \pmod{11}$ analogously to Lemma 7.2.6; then the corollary is the special case of Lemma 7.2.8 when $N \equiv 0 \pmod{11}$ written in terms of divisibility.

Lemma 7.2.11. *If* $ac \equiv bc \pmod{m}$ *and* $(c, m) = 1$ *then* $a \equiv b \pmod{m}$.

Proof. First, assume $(c, m) = 1$. By Corollary 7.1.11,

$$\begin{aligned} & cx + my = 1, \quad \text{for some } xy \in \mathbb{Z} \\ \implies \quad & cx \equiv 1 \pmod{m}. \end{aligned}$$

So now,

$$\begin{aligned} & ac \equiv bc \pmod{m} \\ \implies \quad & acx \equiv bcx \pmod{m} \\ \implies \quad & a \equiv b \pmod{m}. \end{aligned}$$

□

Corollary 7.2.12. *If* $ac \equiv bc \pmod{m}$ *and* $(c, m) = d$ *then* $a \equiv b \pmod{m/d}$.

Lemma 7.2.13. *If* $m_1, m_2 \in \mathbb{N}$ *such that* $(m_1, m_2) = 1$ *and*

$$\begin{aligned} a &\equiv b \pmod{m_1}, \\ a &\equiv b \pmod{m_2} \end{aligned}$$

then

$$a \equiv b \pmod{m_1 m_2}.$$

Theorem 7.2.14 (Chinese Remainder Theorem). *If* $m_1, m_2, \ldots, m_k \in \mathbb{N}$ *are pairwise coprime, i.e.* $(m_i, m_j) = 1$ *for* $i \neq j$, *then the* k *simultaneous congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

have a unique solution modulo $M = \prod_{i=1}^{k} m_i$.
Moreover, the solution may be constructed as follows.

- *Define* $M_i := \prod_{j \neq i} m_j = M/m_i$, *for* $i = 1, 2, \ldots, k$.
- *Define* b_i *to be the multiplicative inverse of* M_i *modulo* m_i, *for each* i, *i.e.*

  $$b_i M_i \equiv 1 \pmod{m_i}, \text{ for } i = 1, 2, \ldots, k,$$

  noting that: $b_i M_i \equiv 1 \pmod{m_i} \iff b_i M_i + q m_i = 1$ *for some integer* $q \in \mathbb{Z}$, *so that* b_i *(and* q*) can be constructed via the Euclidean Algorithm.*
- *The solution is now given by:* $x \equiv \sum_{j=1}^{k} a_j b_j M_j \pmod{M}$.

Proof. The solution above means that, for some $q \in \mathbb{Z}$,

$$x = \sum_{j=1}^{k} a_j b_j M_j + qM.$$

Consider this expression modulo m_i. Since $m_i \mid M_j$ when $j \neq i$, $b_i M_i \equiv 1 \pmod{m_i}$, and $m_i \mid M$ for all i, we have

$$\begin{aligned} x &= \sum_{j=1}^{k} a_j b_j M_j + qM \\ &= \sum_{j \neq i} a_j b_j M_j + a_i b_i M_i + qM \\ &\equiv \sum_{j \neq i} a_j b_j \cdot 0 + a_i \cdot 1 + q \cdot 0 \pmod{m_i} \\ &\equiv a_i \pmod{m_i} \end{aligned}$$

i.e. the expression for x reduces to each of the given congruences. Hence the constructed expression for x satisfies all the given congruences. □

Euler's Totient Function

Definition 7.2.15. For a given natural number n, let the set $\mathcal{S}_n$ of natural numbers $k < n$ that are coprime to n, i.e.

$$\mathcal{S}_n = \{k \in \mathbb{N} \mid k < n \text{ and } (k, n) = 1\}.$$

Then **Euler's totient function** $\varphi(n)$ is defined to be the *cardinality* of $\mathcal{S}_n$.

Example 7.2.16. *For $n = 12$, the set of natural numbers less than n is*

$$\{1, 2, \ldots, 11\}.$$

Eliminating all the elements that are divisible by 2 or 3 (the prime divisors of 12), we have

$$\mathcal{S}_{12} = \{1, 5, 7, 11\},$$

and so

$$\varphi(12) = |\,\mathcal{S}_{12}\,| = 4.$$

In Definition 14.1.1 we define an *abelian group*. In Number Theory, we have some key examples of *abelian groups*.

Example 7.2.17. *$(\mathbb{Z}, +)$ is an abelian group, i.e. the set $\mathbb{Z}$ of integers, with ordinary addition $+$ as the binary operation, is an abelian group.*
Below, we do a "run-through check" that the axioms hold.

G1: $\forall m, n \in \mathbb{Z}$, we have $m + n \in \mathbb{Z}$.

G2: $\forall \ell, m, n \in \mathbb{Z}$, we have $\ell + (m + n) = (\ell + m) + n$.

G3: The identity is 0, since $\forall m \in \mathbb{Z}, 0 + m = m + 0 = m$.

G4: The inverse of each $m \in \mathbb{Z}$ is $-m$ since $m + (-m) = (-m) + m = 0$.

G5: $\forall m, n \in \mathbb{Z}$, we have $m + n = n + m$.

Example 7.2.18. $(\mathcal{S}_n, \cdot)$ *where* $\cdot$ *is multiplication* modulo n *is an abelian group.*

When $n = p$ prime, we get the following special case of Example 7.2.18 is the following, which we need later for Theorem 7.2.33.

Example 7.2.19. *The set* $\mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$ *is an abelian group under multiplication modulo* p*, where* p *is a prime.*

Definition 7.2.20. The **order of a group** G is the number of elements it contains, and is denoted by $|G|$ (essentially, $|G|$ is the cardinality of G when regarded as a set).
The **order of an element** x of a group G is the least number of times that it can be composed with itself to obtain the identity. The order of x is similarly denoted by $|x|$. If the group operation is $\cdot$, in which case the identity is usually represented by 1, then $|x|$ is the least $m \in \mathbb{N}$ for which $x^m = 1$ in G.

Theorem 7.2.21. *If* $(G, \cdot)$ *is a finite group and* $x \in G$ *then* $|x| \,|\, |G|$.

Corollary 7.2.22. *If* $(G, \cdot)$ *is a finite group and* $x \in G$ *then* $x^{|G|} = 1$.

One of the main applications of Euler's totient function is the following generalisation of a theorem we have yet to meet: Fermat's Little Theorem.

Theorem 7.2.23 (Euler's Theorem). *If* $a \in \mathbb{Z}$, $n \in \mathbb{N}$ *and* $(a, n) = 1$, *then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Proof. Using the information in the dangerous bend, $\mathcal{S}_n$ is an abelian group under multiplication *modulo* n, and so Corollary 7.2.22 gives

$$a^{|\,\mathcal{S}_n\,|} \equiv 1 \pmod{n},$$

and the result follows. □

Example 7.2.24. *We have* $(3, 8) = 1$ *and since* $\mathcal{S}_8 = \{1, 3, 5, 7\}$ *is the set of natural numbers less than* 8 *that are coprime to* 8*, we have* $\varphi(8) = |\,\mathcal{S}_8\,| = 4$.
Thus Euler's Theorem tells us $3^4 \equiv 1 \pmod 8$, and indeed we have: $3^4 = 81 \equiv 1 \pmod 8$.

We now obtain a formula for $\varphi(m)$, which depends on two essential properties:

(i) $\varphi(p^k) = p^k - p^{k-1}$, if $k \in \mathbb{N}$ and p is prime;

(ii) φ is a *multiplicative* function (we define what this means below, but we won't bother to prove it).

Definition 7.2.25. A function $f : \mathbb{N} \to \mathbb{N}$ is said to be **multiplicative** if for $a, b \in \mathbb{N}$,

$$(a, b) = 1 \implies f(ab) = f(a)f(b).$$

Theorem 7.2.26. φ *is multiplicative, i.e. if* $m_1, m_2 \in \mathbb{N}$ *then*

$$\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2).$$

Example 7.2.27. *Let's find $\varphi(12)$ using the two properties:*

$$\begin{aligned}\varphi(12) &= \varphi(3)\varphi(4), && \text{by property (ii), since } (3,4)=1\\ &= (3-3^0)(2^2-2^1), && \text{by property (i), twice}\\ &= 2\cdot 2 = 4\end{aligned}$$

as we observed before.

The elements of $\mathcal{S}_p = \{1, 2, \ldots, p-1\}$ are all coprime to p, if p is prime. So it follows immediately that for a prime p, $\varphi(p) = p-1$. We can generalise this idea to get a proof of property (i).

Theorem 7.2.28. *If $n = p^k$ where p is a prime and $k \in \mathbb{N}$ then*

$$\varphi(n) = p^k - p^{k-1} = p^k\Big(\frac{p-1}{p}\Big).$$

Proof. Observe that for a number in $\{1, 2, \ldots, p^k\}$ not to be coprime to $n = p^k$, it must have p as a divisor. So the set $\mathcal{S}_{p^k}$ of natural numbers less than p that are coprime to $n = p^k$ can be written as

$$\mathcal{S}_{p^k} = \{1, 2, \ldots, p^k\} \setminus \big\{pm \mid m \in \{1, 2, \ldots, p^{k-1}\}\big\}.$$
$$\therefore \varphi(n) = |\,\mathcal{S}_{p^k}\,| = p^k - p^{k-1}.$$ □

Theorem 7.2.29. *If N has prime factorisation*

$$N = \prod_{i=1}^{n} p_i^{\varepsilon_i}$$

then

$$\varphi(N) = N\prod_{i=1}^{n}\frac{p_i-1}{p_i}.$$

Proof. This follows by induction on n. □

Example 7.2.30. $\varphi(180) = \varphi(2^2 3^2 5) = 180\Big(\frac{2-1}{2}\Big)\Big(\frac{3-1}{3}\Big)\Big(\frac{5-1}{5}\Big) = 48.$

The following theorem follows from Euler's Theorem as a special case since $\varphi(p) = p-1$, if p is prime, but we give an independent proof.

Theorem 7.2.31 (Fermat's Little Theorem). *If $n \in \mathbb{N}$, p is a prime and $p \nmid n$ then*

$$n^{p-1} \equiv 1 \pmod{p}.$$

Proof. Suppose $r \in \mathbb{Z}$ such that $0 < r < p$. Then $rn \equiv s \pmod{p}$ for some $s \in \mathbb{Z}$, also satisfying $0 < s < p$ (since $rn \equiv 0 \pmod{p}$ would imply $p \mid n$ contrary to assumption). Furthermore, for distinct values of r we obtain different values of s, since if

$$r_1 n \equiv s \pmod{p} \quad \text{and} \quad r_2 n \equiv s \pmod{p},$$

then $r_1 n \equiv r_2 n \pmod{p}$ whence $r_1 = r_2$ by Lemma 7.2.11. Hence

$$1n \cdot 2n \cdot 3n \cdots (p-1)n \equiv 1\cdot 2\cdot 3\cdots(p-1) \pmod{p}$$

which on cancellation (using Lemma 7.2.11) gives

$$n^{p-1} \equiv 1 \pmod{p}.$$ □

Corollary 7.2.32. *If $n \in \mathbb{N}$, p is a prime then $n^p \equiv n \pmod{p}$.*

Proof. If $p \nmid n$ then the result follows from Fermat's Little Theorem by multiplying both sides of the congruence by n. Otherwise $n \equiv 0 \pmod{p}$, in which case the result is trivially true. □

Theorem 7.2.33 (Wilson's Theorem). *Let $1 < n \in \mathbb{N}$. Then*

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ is prime.}$$

Proof. ($\Longrightarrow$) Suppose that $(n-1)! \equiv -1 \pmod{n}$ and let $d \in \mathbb{Z}$ such that $1 \leqslant d \,|\, n$. Then $d \in \{1, 2, \ldots, n-1\}$ and hence

$$d \,|\, (n-1)!.$$

By the congruence, we have $(n-1)! + 1 \equiv 0 \pmod{n}$. Hence, we also have

$$d \,|\, n \,|\, (n-1)! + 1.$$

Hence $d \,|\, 1 = \big((n-1)! + 1\big) - (n-1)!$, and so $d = 1$, which implies n has no **proper divisors**[†], so that n is prime.
($\Longleftarrow$) Suppose $n = p$ prime. Consider $G = \mathbb{Z}_p \setminus \{0\} = \{1, 2, \ldots, p-1\}$ as a group under multiplication modulo p.

Case 1: $p = 2$. Then

$$(p-1)! \equiv 1 \equiv -1 \pmod{2}.$$

Case 2: $p \geqslant 3$. Then p is odd. Each element $a \in G$ has an inverse b, so that we have $ab \equiv 1 \pmod{p}$. First consider the case, $a = b$.

$$\begin{aligned} \Longrightarrow \quad & a^2 \equiv 1 \pmod{p} \\ \Longrightarrow \quad & a^2 - 1 \equiv 0 \pmod{p} \\ \Longrightarrow \quad & (a-1)(a+1) \equiv 0 \pmod{p} \end{aligned}$$

So that we have $a \equiv \pm 1 \pmod{p} \implies a = 1$ or $a = p-1$. Otherwise we have $a \neq b$. Thus except for 1 and $p-1$, the elements of G can be collected in pairs whose product is 1, so that

$$\begin{aligned} (p-1)! &\equiv 1^{(p-3)/2} \cdot 1 \cdot (p-1) \pmod{p} \\ &\equiv (p-1) \pmod{p} \\ &\equiv -1 \pmod{p} \end{aligned}$$

So in all cases, $(n-1)! \equiv -1 \pmod{n}$. □

[†]**Definition.** If $d \in \mathbb{N}$ then d is a **proper divisor** of n if $d \,|\, n$ and $1 < d < n$.

Exercise Set 7.

1. For each of the following pairs of integers a, b use the *Euclidean Algorithm* to find $d = (a, b)$ and find a pair of integers x, y such that $ax + by = d$.

   (i) $a = 85$, $b = 41$; (ii) $a = 2613$, $b = 637$.

2. Show that if there exist integers x, y such that $ax + by = 1$ then $(a, b) = 1$.

3. Show that $(3k + 2, 5k + 3) = 1$ for any integer k.

4. Show that $(a, a + 2) = 2$ if a is even and $(a, a + 2) = 1$ otherwise.

5. Show that if $(a, b) = 1$ then $(a + b, a - b) = 1$ or 2.

6. Find all solutions to the following *Diophantine Equations*.

   (i) $2x + 5y = 11$. (ii) $12x + 18y = 50$. (iii) $202x + 74y = 7638$.

   Does equation (iii) have a solution in *positive* integers x, y?

7. A grocer orders apples and oranges at a total cost of \$8.39. If apples cost 25c each and oranges cost 18c each, how many of each type of fruit did the grocer order?

8. An apartment block has units at two rates: most rent at \$87/week, but a few rent at \$123/week. When all are rented the gross income is \$8733/week. How many units of each type are there?

∗9. When Jane is one year younger than Betty will be when Jane is half as old as Betty will be when Jane is twice as old as Betty is now, Betty will be three times as old as Jane was when Betty was as old as Jane is now.
One is in her teens and ages are in completed years. How old are they?

10. Solve the adjacent *alphametic* (an addition in which: each letter stands for a different digit; and left-most digits of a number are not allowed to be 0).

$$\begin{array}{cccc} & A & H & A \\ & A & H & A \\ & & & A \\ & W & A & G \\ \hline H & A & H & A \end{array}$$

   Answer. HAHA = 1717 ($W = 2$, $G = 6$). The solution is unique.

11. About all we know of Diophantus' life is his epitaph from which his age at death is to be deduced:

    > Diophantus spent one-sixth of his life in childhood, one-twelfth in youth, and another one-seventh in bachelorhood. A son was born five years after his marriage and died four years before his father at half his father's age.

12. Augustus de Morgan, a nineteenth-century mathematician, stated:

    > I was x years old in the year x^2.

    When was he born?

13. Prove that for every integer n:

    (i) $3 \mid n^3 - n$; (iii) $7 \mid n^7 - n$;
    (ii) $5 \mid n^5 - n$; (iv) $11 \mid n^{11} - n$.

    Show that $n^9 - n$ is not necessarily divisible by 9. *Hint:* Try $n = 2$.
    What general result is suggested by the above?

14. Prove that $3^{6n} - 2^{6n}$ is divisible by 35, for every positive integer n.

∗15. What is the final digit of $7^{7^{7^{7^{7^7}}}}$.

Exponentiation convention. Note that a^{b^c} means $a^{(b^c)}$. Mathematicians chose the "from the right" definition, since

$$(a^b)^c = a^{bc},$$

i.e. the "from the left" expression can be written without power towers and without brackets.

16. Prove that for any $n \in \mathbb{N}$, 17 divides $2^n.3^{2n} - 1$.

17. Prove that for any $n \in \mathbb{N}$, $17^n - 12^n - 24^n + 19^n$ is divisible by 35.

18. Using Fermat's Little Theorem, prove that for all positive integers a and b:

    (i) 3 divides $(a+b)^3 - a^3 - b^3$; (ii) 5 divides $(a+b)^5 - a^5 - b^5$.

∗19. Prove that $5^{99} + 11^{99} + 17^{99}$ is divisible by 33.

∗20. What is the final digit of $((((((((((7^7)^7)^7)^7)^7)^7)^7)^7)^7)^7)$? (7 occurs as a power 10 times.)

∗21. *(17th International Olympiad, 1975, Problem 4)* When 4444^{4444} is written in decimal notation, the sum of its digits is A. Let B be the sum of the digits of A. Find the sum of the digits of B.
Hints: First show that the sum of the digits of B is fairly small (in fact: less than 16). Then use the fact that, for any natural number N,

$$N \equiv (\text{sum of the digits of } N) \pmod 9.$$

22. Show $7 \mid 2222^{5555} + 5555^{2222}$.

23. For which a does the congruence $ax \equiv 1 \pmod m$ have a solution, when ...

    (i) $m = 4$? (ii) $m = 5$? (iii) $m = 6$? (iv) $m = 7$?

24. Solve $58x \equiv 1 \pmod{127}$.
    [*Hint.* Use the Euclidean Algorithm as one of your steps.]

25. Use Wilson's Theorem to show that $(p-1)! \equiv p - 1 \pmod{p(p-1)}$ if p is prime.

26. Find the remainder when 97! is divided by 101.