2 Divisibility, Primes & Unique Factorization

The main goal of this chapter is to develop the *Fundamental Theorem of Arithmetic*, or *Unique Factorization Theorem*, which states that every integer ≥ 2 can be written uniquely as a product of primes, e.g.,

$$36 = 2^2 \cdot 3^2, \qquad 986 = 2 \cdot 17 \cdot 29, \qquad 10001 = 73 \cdot 137$$

As a precursor, we review some material which you should have encountered in a previous course.

2.1 The Greatest Common Divisor and the Euclidean Algorithm

Our first definition recalls and extends the idea of divisibility seen in the Introduction.

Definition 2.1. Let a, b, d be integers: if $d \mid a$ and $d \mid b$ then d is a *common divisor*[a] of a and b.

If a and b are not both zero, then the *greatest common divisor* of a, b is written $d = \gcd(a, b)$.

We say that a and b are *coprime* or *relatively prime* if $\gcd(a, b) = 1$.

[a] By convention one tends to list only *positive* common divisors.

Since there are finitely many positive common divisors (all satisfy $d \leq \max(|a|, |b|)$) $\gcd(a, b)$ must therefore exist. The definition may be extended to any list of numbers: $\gcd(a_1, \ldots, a_n)$ is the largest divisor of all the numbers $a_1, \ldots, a_n$.

Examples 2.2. $\gcd(0, 9) = 9$, $\gcd(45, 33) = 3$, $\gcd(162, 450) = 18$.

Our first goal is to develop an algorithm to efficiently compute gcd's. This starts with the notion of division in the integers.

Theorem 2.3 (Division algorithm). *If $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exist unique $q, r \in \mathbb{Z}$ (the* quotient *and* remainder*) such that*

$$a = qb + r, \quad 0 \leq r < b$$

Example 2.4. The division algorithm should reminder you of elementary school math!

$$\left.\begin{array}{r} 13 \div 4 = 3\,\mathrm{r}\,1 \\ b \div a = q\,\mathrm{r}\,r \end{array}\right\} \iff \left\{\begin{array}{r} 13 = 3 \cdot 4 + 1 \\ a = q \cdot b + r \end{array}\right.$$

Proof. Consider the set $S = \mathbb{N}_0 \cap \{a - bz : z \in \mathbb{Z}\}$. This is a non-empty (e.g. take $z = -|a|$) subset of the natural numbers, whence (well-ordering) it has a minimum element $r \in S$.

Certainly $r \in [0, b)$ for otherwise $r - b \in S$ contradicts the minimality of r. Now let $q = \frac{a-r}{b}$ be the corresponding choice of z to establish existence.

For uniqueness, suppose that $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1, r_2 < b$. Then

$$-b < r_1 - r_2 < b \quad \text{and} \quad r_1 - r_2 = (q_2 - q_1)b$$

Thus $r_1 - r_2$ is divisible by b and lies in the interval $(-b, b)$. Clearly $r_2 = r_1$, whence $q_2 = q_1$ and we have uniqueness. ∎

Is it really an *algorithm*? The presentation of Theorem 2.3 doesn't seem very algorithmic: indeed we simply take it as given that we can find q, r by whatever means we wish (messing with a calculator is fine!). To see it more as an algorithm, consider the case where $a > 0$ and follow these instructions:

1. Is $a < b$? If Yes, stop: $r = a$ and $q = 0$.
2. Otherwise, compute $a - b$.
3. Is $a - b < b$? If Yes, stop: $r = a - b$ and $q = 1$.
4. Otherwise, compute $a - 2b$, etc.
5. Repeat until the process terminates.

Simple code

```
int a=240; int b=7;
int q=0; int r=a;
while(r>=b){r=r-b; q=q+1;}
write(q,r);
```

The simple program computes $q = 34$ and $r = 2$ from $a = 240$ and $b = 7$ by repeatedly subtracting 7 from 240 until it can no longer do so. You can check that $240 = 34 \cdot 7 + 2$. If you like, you can paste and edit the code here.

The Euclidean Algorithm For us, the beauty of the division algorithm is that it transfers the gcd of one pair of numbers to another. For instance, dividing $57 \div 12$ we see that

$$57 = 4 \cdot 12 + 9 \quad \text{and} \quad \gcd(57, 12) = 3 = \gcd(12, 9)$$

More generally, suppose $a = bq + r$. Plainly, a and b are both divisible by $\gcd(b, r)$. Since any common divisor of a, b can be no larger than the greatest such;

$$\gcd(b, r) \le \gcd(a, b)$$

By symmetry $r = a - bq \implies \gcd(a, b) \le \gcd(b, r)$, and we conclude:

Lemma 2.5. *If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.*

If $a, b > 0$, we may therefore compute $\gcd(a, b)$ by repeatedly invoking the division algorithm until we obtain a remainder $r_{k+1} = 0$: this process is the *Euclidean algorithm.*

$$\begin{array}{lll}
\text{(Line 1)} & a = q_1 b + r_1 & 0 \le r_1 < b \\
\text{(Line 2)} & b = q_2 r_1 + r_2 & 0 \le r_2 < r_1 \\
\text{(Line 3)} & r_1 = q_3 r_2 + r_3 & 0 \le r_3 < r_2 \\
 & \quad \vdots & \\
\text{(Line } k\text{)} & r_{k-2} = q_k r_{k-1} + r_k & 0 \le r_k < r_{k-1} \\
\text{(Line } k+1\text{)} & r_{k-1} = q_{k+1} r_k + 0 &
\end{array}$$

Theorem 2.6. *The Euclidean algorithm terminates with final non-zero remainder $r_k = \gcd(a, b)$.*

Proof. *A decreasing sequence of positive integers* $b > r_1 > r_2 > r_3 > \cdots > 0$ takes *at most* b steps to reach 0 (in practice far fewer), whence the algorithm terminates in at most b steps.

Finally, by Lemma 2.5,

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k) = \gcd(r_k q_{k+1}, r_k) = r_k$$

■

If a or b are negative, simply apply the algorithm to the pair $|a|, |b|$.

Example 2.7. We use the algorithm[a] to compute $\gcd(161,140)$

$$\left.\begin{aligned}\mathbf{161} &= 1\cdot\mathbf{140}+\mathbf{21}\\ \mathbf{140} &= 6\cdot\mathbf{21}+\mathbf{14}\\ \mathbf{21} &= 1\cdot\mathbf{14}+\mathbf{7}\\ \mathbf{14} &= 2\cdot\mathbf{7}\end{aligned}\right\} \implies \gcd(161,140)=7$$

We could instead have evaluated $\gcd(161,140)$ by listing the positive divisors of 140 (namely 1, 2, 4, 5, 7, 10, 14, 20, 28, 35, 70, 140) and checking which of these is also a divisor of 161. For larger a,b, finding all the divisors is prohibitively time-consuming, whereas the Euclidean algorithm will always do the job in a (relatively) efficient manner.

To motivate the next result, we now reverse the algorithm to express the gcd as a linear combination of the original pair $(161,140)$:

$$\begin{aligned}\mathbf{7} &= \mathbf{21}-1\cdot\mathbf{14} && \text{(rearrange line 3)}\\ &= \mathbf{21}-(\mathbf{140}-6\cdot\mathbf{21}) && \text{(substitute for } \mathbf{r}_2=\mathbf{14} \text{ using line 2)}\\ &= -\mathbf{140}+7\cdot\mathbf{21}\\ &= -\mathbf{140}+7\cdot(\mathbf{161}-\mathbf{140}) && \text{(substitute for } \mathbf{r}_1=\mathbf{21} \text{ using line 1)}\\ &= 7\cdot\mathbf{161}-8\cdot\mathbf{140}\end{aligned}$$

[a] Remainders are in boldface for clarity. We also do this in the next proof. Consider underlining when writing by hand to help avoid mistakes. Observe how one can trace the same remainder diagonally $\swarrow$.

The reversal of the algorithm seen in the example is hugely important and can be done in general.

Theorem 2.8 (Extended Euclidean Algorithm/Bézout's Identity). *Suppose that $a,b\in\mathbb{Z}$ are not both zero. Then there exist integers x,y such that*

$$\gcd(a,b)=ax+by$$

There are a great many existence theorems in Mathematics, but few of them tell you explicitly how to construct the desired objects.

Proof. Suppose $a,b>0$ and that we've applied the Euclidean algorithm to obtain $r_k=\gcd(a,b)$. Rearrange the penultimate line and repeatedly move up the algorithm using each line to substitute for the smallest remainder:

$$\begin{aligned}\mathbf{r}_k &= \mathbf{r}_{k-2}-q_k\mathbf{r}_{k-1} && \text{(line } k\text{)}\\ &= \mathbf{r}_{k-2}-q_k(\mathbf{r}_{k-3}-q_{k-1}\mathbf{r}_{k-2})=(1+q_{k-1}q_k)\mathbf{r}_{k-2}-q_k\mathbf{r}_{k-3} && \text{(line } k-1\text{)}\\ &= (1+q_{k-1}q_k)(\mathbf{r}_{k-4}-q_{k-2}\mathbf{r}_{k-3})-q_k\mathbf{r}_{k-3}=(\cdots)\mathbf{r}_{k-3}+(\cdots)\mathbf{r}_{k-4} && \text{(line } k-2\text{)}\\ &\ \vdots\\ &= (\cdots)\mathbf{b}+(\cdots)\mathbf{r}_1 && \text{(line 2)}\\ &= (\cdots)\mathbf{a}+(\cdots)\mathbf{b} && \text{(line 1)}\end{aligned}$$

Each omitted term $(\cdots)$ is plainly an integer, obtained by adding and multiplying the quotients q_j. If either a or b is negative, compute with $|a|, |b|$ and adjust ±-signs accordingly. ■

Example 2.9. Find $d = \gcd(1132, 490)$ and integers x, y such that $d = 1132x + 490y$.
Simply apply the algorithm:

$$\left.\begin{aligned} \mathbf{1132} &= 2\cdot\mathbf{490}+\mathbf{152}\\ \mathbf{490} &= 3\cdot\mathbf{152}+\mathbf{34}\\ \mathbf{152} &= 4\cdot\mathbf{34}+\mathbf{16}\\ \mathbf{34} &= 2\cdot\mathbf{16}+\mathbf{2}\\ \mathbf{16} &= 8\cdot\mathbf{2} \end{aligned}\right\} \implies \gcd(1132,490)=2$$

Now reverse the steps:

$$\begin{aligned} \mathbf{2} &= \mathbf{34} - 2\cdot\mathbf{16} && \text{(line 4)}\\ &= \mathbf{34} - 2\cdot(\mathbf{152}-4\cdot\mathbf{34}) = 9\cdot\mathbf{34}-2\cdot\mathbf{152} && \text{(line 3)}\\ &= 9\cdot(\mathbf{490}-3\cdot\mathbf{152})-2\cdot\mathbf{152} = 9\cdot\mathbf{490}-29\cdot\mathbf{152} && \text{(line 2)}\\ &= 9\cdot\mathbf{490}-29\cdot(\mathbf{1132}-2\cdot\mathbf{490}) = 67\cdot\mathbf{490}-29\cdot\mathbf{1132} && \text{(line 1)} \end{aligned}$$

Hence $(x, y) = (-29, 67)$ is a solution to $d = 1132x + 490y$.

As an example of the immediate theoretical power of Theorem 2.8 we prove the following:

Corollary 2.10. *If a, b are coprime and $a \mid bc$, then $a \mid c$.*

Proof. Since $\gcd(a, b) = 1$, $\exists x, y \in \mathbb{Z}$ such that

$$1 = ax + by \implies c = acx + bcy$$

This last is divisible by a by assumption. ∎

Now we apply Bézout to obtain an important visualization of $\gcd(a, b)$.

Corollary 2.11. *Suppose $a, b \in \mathbb{Z}$ are not both zero and $d = \gcd(a, b)$. Then*

$$\{ax + by : x, y \in \mathbb{Z}\} = \{md : m \in \mathbb{Z}\}$$

Plainly d is the least positive member of this set.

Proof. Write $D = \{ax + by : x, y \in \mathbb{Z}\}$ and $M = \{md : m \in \mathbb{Z}\}$.
$(D \subseteq M)$ Certainly $d \mid ax + by$ for all $x, y \in \mathbb{Z}$, whence every element of D is a multiple of d.
$(M \subseteq D)$ By Bézout's identity, $d = aX + bY$ for some $X, Y \in \mathbb{Z}$, and so $d \in D$. It follows that

$$md = a(mX) + b(mY) \in D$$

∎

In more advanced treatments involving rings other than the integers, Corollary 2.11 is often used as the *definition* of $\gcd(a, b)$. This has the advantage of permitting one to define the gcd without first requiring a Euclidean algorithm: many more rings have a gcd than have a Euclidean algorithm!

Linear Diophantine Equations

As a simple application, we consider integer solutions x, y to equations $ax + by = c$ where $a, b, c \in \mathbb{Z}$ are given. Bézout's identity tells us how to find a solution whenever $c = \gcd(a, b)$. With the help of Corollary 2.11, this is essentially all we need.

Corollary 2.12. *The Diophantine equation $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$.*

Proof. A solution exists $\iff c \in \{ax + by : x, y \in \mathbb{Z}\} \iff c$ is a multiple of $\gcd(a, b)$. ∎

Example 2.13. Show that $147x - 45y = 2$ has no solutions in integers.

$$\left.\begin{aligned} \mathbf{147} &= 3 \cdot \mathbf{45} + \mathbf{12} \\ \mathbf{45} &= 3 \cdot \mathbf{12} + \mathbf{9} \\ \mathbf{12} &= 1 \cdot \mathbf{9} + \mathbf{3} \\ \mathbf{9} &= 3 \cdot \mathbf{3} \end{aligned}\right\} \implies \gcd(147, 45) = 3 \nmid 2$$

Now let $d = \gcd(a, b)$ and suppose that $d \mid c$ so that we have a solution (x_0, y_0) to $ax + by = c$. Consider $(x, y) = (x_0 + x_h, y_0 + y_h)$ and observe that[1]

$$\begin{aligned} ax + by = c &\iff c = a(x_0 + x_h) + b(y_0 + y_h) = c + ax_h + by_h \\ &\iff ax_h + by_h = 0 \iff \frac{b}{d} y_h = -\frac{a}{d} x_h \end{aligned}$$

Since $\frac{a}{d}, \frac{b}{d}$ are *coprime integers*, Corollary 2.10 shows that $\frac{b}{d}$ divides x_h. This is enough to prove:

Corollary 2.14. *Let $d = \gcd(a, b)$ and suppose (x_0, y_0) is a solution to the Diophantine equation $ax + by = c$. Then all solutions may be found via*

$$(x, y) = \left(x_0 + \frac{b}{d} t, y_0 - \frac{a}{d} t \right) \quad \textit{where} \quad t \in \mathbb{Z}$$

Examples 2.15. 1. Find all the solutions to the Diophantine equation $161x + 140y = -14$.

By Example 2.7 we have $d = \gcd(161, 140) = 7$ and a solution $(7, -8)$ to $161x + 140y = 7$. Multiply by -2 to obtain a suitable (x_0, y_0) and apply the Theorem

$$(x, y) = \left(-14 + \frac{140}{7} t, 16 - \frac{161}{7} t \right) = (-14 + 20t, 16 - 23t) : t \in \mathbb{Z}$$

2. Find all solutions in integers to the equation $490x - 1132y = 4$.

By Example 2.9, we know that $d = \gcd(1132, 490) = 2$ and that $(-29, 67)$ is a solution to $1132x + 490y = 2$. Rearranging and taking ±-signs into account, we see that $(x_0, y_0) = (134, 58)$ is a solution to the equation of interest. The general solution is therefore

$$(x, y) = \left(134 + \frac{1132}{2} t,\ 58 + \frac{490}{2} t, \right) = (134 + 566t,\ 58 + 245t) : t \in \mathbb{Z}$$

[1] We use (x_h, y_h) since this solves the associated *homogeneous* equation $ax_h + by_h = 0$. The method of solution is analogous to solving non-homogeneous linear ordinary differential equations and linear algebra problems $A\mathbf{x} = \mathbf{b}$.

Exercises 2.1 1. Verify the following elementary properties of divisibility, where a, b, c are integers.

(a) $a \mid 0$, $a \mid a$ and $\pm 1 \mid a$.

(b) If $a \mid b$ and $b \mid c$, then $a \mid c$ (divides is *transitive*).

(c) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for all $x, y \in \mathbb{Z}$.

2. Use the Euclidean Algorithm to compute the following (*use a calculator!*)

(a) $\gcd(121, 105)$ (b) $\gcd(12345, 67890)$ (c) $\gcd(54321, 9876)$

3. Evaluate $\gcd(4655, 12075)$ in the form $12075x + 4655y$ where $x, y \in \mathbb{Z}$.

4. Find all the integer solutions (if any exist) to the following equations.

(a) $4x - y = 7$ (b) $12x + 4y = 10$ (c) $105x - 121y = 1$

(d) $2072x + 1813y = 2849$ (e) $12345x - 67890y = \gcd(12345, 67890)$

(f) $\begin{cases} 7x + 2y = 21 \\ 3x - 7z = 2 \end{cases}$ (use the method several times)

5. Find all solutions of $19x + 20y = 1909$ with $x > 0$ and $y > 0$.

6. Let $r_0, r_1, r_2, \ldots$ be the successive remainders in the Euclidean Algorithm applied to $a > b > 0$ (take $b = r_0$). Show that every two steps reduces the remainder by at least one half: i.e.,

$$r_{i+2} < \frac{1}{2} r_i \quad \forall i = 0, 1, 2, 3 \ldots$$

Conclude that the Euclidean algorithm terminates in at most $2 \log_2 b$ steps. In particular, show that the number of steps is at most seven times the number of digits in b.

7. The *Fibonacci numbers* $(F_n)_{n=1}^{\infty} = (1, 1, 2, 3, 5, 8, 13, \ldots)$ are defined by the recurrence relation

$$\begin{cases} F_{n+2} = F_{n+1} + F_n, \ \forall n \in \mathbb{N}, \\ F_1 = F_2 = 1 \end{cases}$$

(a) Prove that no two successive Fibonacci numbers have a common divisor $a > 1$.

(b) Use the Euclidean algorithm to verify $\gcd(F_7, F_6) = \gcd(13, 8) = 1$. Repeat for $\gcd(F_8, F_7)$.

(c) Make a hypothesis about how many steps are necessary in order to compute $\gcd(F_{n+1}, F_n)$.

(d) Compute $2 \log_2 F_n$ for $n = 4, 5, 6, 7, 8$. Considering question 6, why might we say that the Euclidean algorithm is very *slow* when applied to successive Fibonacci numbers?

8. Let a, b, r, s be given constants. Prove that the arithmetic progressions

$$\{ax + r : x \in \mathbb{Z}\} \quad \text{and} \quad \{by + s : y \in \mathbb{Z}\}$$

intersect if and only if $\gcd(a, b) \mid (s - r)$.

9. Show that if $ad - bc = \pm 1$, then the fraction $\frac{a+b}{c+d}$ is in reduced form (i.e. $\gcd(a + b, c + d) = 1$).

10. Show that if $\gcd(a, b) = 1$, then $\gcd(a - b, a + b) = 1$ or 2. Exactly when is the value 2?

2.2 Primes and Unique Factorization

Now we turn to the building blocks of the integers, the prime numbers. The very idea that the primes are 'building blocks' is a colloquial expression of a famous result, examples of which are on page 1.

Theorem 2.16 (Fundamental Theorem of Arithmetic/Unique Prime Factorization). *Every integer z is either zero, ± 1, or may be uniquely factored in the form*

$$z = u p_1^{\mu_1} \cdots p_n^{\mu_n}$$

where $u = \pm 1$, $p_1 < \cdots < p_n$ are primes and each $\mu_i \in \mathbb{N}$.

The first question is obvious: *what is a prime*? You should have previously encountered two suitable notions, though algebraically they present quite differently.

Definition 2.17. An integer $z \geq 2$ is said to be:[a]

Prime if whenever it divides a product, it divides one of the factors: $z \mid ab \implies z \mid a$ or $z \mid b$

Irreducible if its only positive divisors are 1 and itself: $\forall k \in \mathbb{N},\ k \mid z \implies k = 1$ or z.

Composite if it is not irreducible: $\exists a, b \in \mathbb{N}$ such that $z = ab$ and $2 \leq a, b < z$.

[a] A note for algebraists who might have seen these definitions elsewhere. We follow the convention in the integers that primes, irreducibles and composites must be *positive*. A more formal algebraic definition allows, say -5 to be prime/irreducible. More properly, if z is prime/irreducible in a ring, so is uz where u is a *unit*: the only units in the ring of integers are ± 1.

Examples 2.18. 1. The integer $z = 5$ is prime/irreducible:

Prime: for example $5 \mid (15 \cdot 11)$ and $5 \mid 15$.

Irreducible: its only positive divisors are 1 and 5.

2. The integer $z = 4$ is not prime & composite:

Not prime: for example $4 \mid (6 \cdot 10)$ but $4 \nmid 6$ and $4 \nmid 10$.

Composite: the positive divisors are 1, 2 and 4.

The distinction between primes and irreducibles is partly artificial: the uniqueness proof of the Fundamental Theorem will be seen to hinge on the fact that *primes and irreducibles are identical*! After this section, *prime* will refer to any positive integer satisfying both of the prime/irreducible conditions in Definition 2.17. In abstract algebra however, the distinction is far more important: there exist many rings where primes and irreducibles are genuinely *different* objects.[2]

[2] In a later class, our approach in this section will be seen to generalize to other rings in which primes and irreducibles are identical; in such cases an analogue of the unique factorization theorem can often be produced. This isn't a universal, for in some rings the concepts are distinct and there might exist non-unique factorizations. For those with some experience: all four of $2, 3, \sqrt{10} \pm 2$ are irreducible in the ring $\mathbb{Z}[\sqrt{10}]$, and we have a non-unique irreducible factorization

$$6 = 2 \cdot 3 = (\sqrt{10} - 2)(\sqrt{10} + 2)$$

In this ring, 2 is irreducible but *not* prime: good luck showing this at the moment!

Existence: Irreducibiles and Composites

The first stage of proving the Fundamental Theorem is to factor every positive integer by irreducibles.

Lemma 2.19. *Every composite is divisible by an irreducible.*

Proof. Suppose $z \geq 2$ is composite but has no irreducible factors. Then:

- $z = a_1 b_1$ where $a_1, b_1 \geq 2$ are not irreducible: plainly a_1, b_1 are composites.
- If a_1 had an irreducible factor then this would be an irreducible factor of z. Hence a_1 is composite and may be written $a_1 = a_2 b_2$ for $a_2, b_2 \geq 2$ composite.
- Repeat the process *ad infinitum*:

  $$z = a_1 b_1 = a_2 b_2 b_1 = a_3 b_3 b_2 b_1 = \cdots$$

  Since each $b_n \geq 2$ we see that $(a_1, a_2, a_3, a_4, \ldots)$ is a decreasing sequence of positive integers: contradiction.

■

We can now prove a famous result dating at least back to Euclid (300 BC).

Theorem 2.20. *There are infinitely many irreducibles.*

Proof. Suppose that $p_1, \ldots, p_n$ constitutes all irreducibles and consider $P := p_1 \cdots p_n + 1$. By Lemma 2.19, P has an irreducible factor p which, by assumption, is one of our irreducibles p_i. But then

$$p \mid P \quad \text{and} \quad p \mid p_1 \cdots p_n \implies p \mid 1$$

which contradicts the fact that $p \geq 2$.

■

We also quickly obtain the existence part of the Fundamental Theorem.

Theorem 2.21. *Every integer $z \geq 2$ is a product of irreducibles.*

Proof. This is merely an iteration of Lemma 2.19.

- If z is irreducible, we are done.
- Otherwise, $z = p_1 a_1$ where p_1 is irreducible and $a_1 \in \mathbb{N}$. If a_1 is irreducible, we are done.
- Otherwise, $z = p_1 p_2 a_2$ where p_2 is irreducible and $a_2 \in \mathbb{N}$. If a_2 is irreducible, we are done.
- Continue until the process terminates and we obtain the factorization $z = p_1 p_2 \cdots p_n$.

If the process never terminated, then $(z, a_1, a_2, \ldots)$ would be a sequence of decreasing positive integers; a contradiction.

■

Nothing in the Theorem assists us in *computing* a suitable factorization. The best approach for small integers is simply to hack at it. For large numbers, factorization is a very hard (i.e. slow) problem.

Uniqueness: Primes and Irreducibles are Identical

The existence part of the Fundamental Theorem is really a claim about *irreducibles.* We've said nothing yet about primes.

Lemma 2.22. *In the integers, primes and irreducibles are identical.*

Proof. 1. (Every prime is irreducible) Suppose p is prime and that $p = kl$ where $k, l \in \mathbb{N}$: our goal is to prove that $\{k, l\} = \{1, p\}$.

Since p is prime, we have $p \mid k$ or $p \mid l$. WLOG suppose the former: $k = p\alpha$ for some $\alpha \in \mathbb{Z}$. But then

$$p = p\alpha l \implies \alpha l = 1$$

Since we are working in the integers and $l > 0$, it follows that $kl = \alpha = 1$ and $k = p$.

2. (Every irreducible is prime) Suppose z is irreducible and that $z \mid ab$ where $a, b \in \mathbb{Z}$: our goal is to prove that $z \mid a$ or $z \mid b$.

Let $d = \gcd(a, z)$. Since z is irreducible, there are only two possibilities:

- $d = 1$: in this case $\gcd(a, z) = 1$ and $z \mid ab$ implies (Corollary 2.10) that $z \mid b$.
- $d = z$: in this case $z \mid a$.

■

The first argument used much less technology than the second, which depended crucially on Bézout's identity and the Euclidean algorithm.[3]

The equivalence of irreducibles and primes yields the uniqueness part of the Fundamental Theorem.

Proof of Theorem 2.16. We can factor z into irreducibles by Theorem 2.21. Now suppose we have two distinct such factorizations

$$z = p_1^{\mu_1} \cdots p_n^{\mu_n} = q_1^{\nu_1} \cdots q_m^{\nu_m}$$

Since the factorizations are distinct, at least some terms remain after dividing both sides by all common irreducible factors:

$$p_{n_1}^{\alpha_1} \cdots p_{n_k}^{\alpha_t} = q_{m_1}^{\beta_1} \cdots q_{m_l}^{\beta_l}$$

where $\{p_{n_1}, \ldots, p_{n_k}\}$ and $\{q_{m_1}, \ldots, q_{m_l}\}$ are distinct sets of irreducibles and all $\alpha_i, \beta_j \in \mathbb{N}$.

Plainly the *irreducible* p_{n_1} divides the *right hand side.* Since p_{n_1} is also *prime* (Lemma 2.22) we see that it divides at least one of the irreducibles $q_{m_1}, \ldots, q_{m_l}$. This is a contradiction.

■

[3] For algebra experts, part 1 really only requires that we're working in an *integral domain*:

$$p = p\alpha l \implies p(1 - \alpha l) = 0 \implies \alpha l = 1$$

since an integral domain has no *zero divisors.* The fact that every prime is irreducible is thus highly generalizable. By contrast, the existence of a Bézout-type identity or a Euclidean algorithm is very *rare* in a general ring. The fact that every irreducible is prime is special to the integers and to relatively few other rings.

Simple Consequences of the Fundamental Theorem

Now that we have unique factorization, several 'obvious' things are seen to be true.

Corollary 2.23. *Suppose $a = p_1^{\mu_1} \cdots p_n^{\mu_n}$ and $b = p_1^{\nu_1} \cdots p_n^{\nu_n}$ are written in terms of their unique factorizations.*[a] *Then:*

1. *$b \mid a \iff \nu_i \le \mu_i$ for all i. Essentially, all primes in b must also be in a.*
2. $\gcd(a,b) = p_1^{\min(\mu_1,\lambda_1)} \cdots p_n^{\min(\mu_n,\lambda_n)}$.
3. *a is a perfect square if and only if every μ_i is even (consider $a = b^2$ then $\mu_i = 2\nu_i$).*
4. *$a^2 \mid b^2 \implies a \mid b$.*
5. *If ab is a perfect square and $\gcd(a,b) = 1$, then both a and b are perfect squares.*

[a] Some exponents may need to be zero in order to have the same lists of primes.

The last two statements were used in our discussion of Pythagorean triples.

Definition 2.24. The *least common multiple* $\operatorname{lcm}(a,b)$ of two positive integers a, b is the smallest positive integer divisible by both a and b.

Following the notation in the Corollary,

$$\left.\begin{array}{l} a = p_1^{\mu_1} \cdots p_n^{\mu_n} \\ b = p_1^{\nu_1} \cdots p_n^{\nu_n} \end{array}\right\} \implies \operatorname{lcm}(a,b) = p_1^{\max(\mu_1,\nu_1)} \cdots p_n^{\max(\mu_n,\nu_n)}$$

$$\implies \operatorname{lcm}(a,b) \cdot \gcd(a,b) = ab$$

This last follows since $\max(\mu_i,\lambda_i) + \min(\mu_i,\lambda_i) = \mu_i + \lambda_i$

Warning: this formula *does not hold* for gcd's or lcm's of three or more integers.

Examples 2.25. 1. To find $\operatorname{lcm}(110,154)$, there are three obvious approaches:

(a) Brute force: list several small multiples of each and look for the smallest. This is no fun.

(b) Prime factorizations: if we know that $110 = 2 \cdot 5 \cdot 11$ and $154 = 2 \cdot 7 \cdot 11$, then

$$\operatorname{lcm}(110,154) = 2 \cdot 5 \cdot 7 \cdot 11 = 770$$

(c) Use the Euclidean algorithm:

$$\left.\begin{array}{l} \mathbf{154} = 1 \cdot \mathbf{110} + \mathbf{44} \\ \mathbf{110} = 2 \cdot \mathbf{44} + \mathbf{22} \\ \mathbf{44} = 2 \cdot \mathbf{22} \end{array}\right\} \implies \gcd(110,154) = 22$$

$$\implies \operatorname{lcm}(110,154) = \frac{110 \cdot 154}{22} = 770$$

2. To find $\operatorname{lcm}(4,6,10)$, we use the prime factorizations:

$$\operatorname{lcm}(4,6,10) = \operatorname{lcm}(2^2, 2 \cdot 3, 2 \cdot 5) = 2^2 \cdot 3 \cdot 5 = 60$$

Note that

$$60 = \operatorname{lcm}(4,6,10) \ne \frac{4 \cdot 6 \cdot 10}{\gcd(4,6,10)} = \frac{240}{2} = 120$$

Exercises 2.2 1. Evaluate the following by finding unique prime factorizations: *use a calculator!*

(a) $\operatorname{lcm}(845, 8788)$

(b) $\operatorname{lcm}(825, 495)$

(c) $\operatorname{lcm}(2310, 1870)$

(d) $\operatorname{lcm}(198061, 231896)$

2. Suppose that $\gcd(a, b) = 1$ and let c be an integer.

   (a) Use the prime factorizations of a, b and c to prove the following.

      i. $a \mid bc \implies a \mid c$ (*this is a cheat, since we used it to prove prime factorization!*)

      ii. If $a \mid c$ and $b \mid c$, then $ab \mid c$

      iii. $\gcd(ab, c) = \gcd(a, c) \gcd(b, c)$

      (*It follows that* $\gcd(ab, c) = 1 \iff \gcd(a, c) = 1 = \gcd(b, c)$ *whenever* a, b *are coprime*)

   (b) We proved part (a)(i) in Corollary 2.10 using Bézout's identity. Can you prove (ii) and (iii) similarly; i.e. *without* using unique factorization? (*Warning: (iii) is especially difficult!*)

3. Use Exercise 2 part (a)(iii) to prove that, for all $x, y \in \mathbb{Z}$ we have

$$\gcd(ab, ay + bx) = \gcd(a, x) \gcd(b, y)$$

4. Suppose a, b, c are all non-zero. Prove or disprove:

   (a) $\gcd(a, b) = \gcd(a, c) \implies \gcd(a^2, b^2) = \gcd(a^2, c^2)$

   (b) $\gcd(a, b) = \gcd(a, c) \implies \gcd(a, b) = \gcd(a, b, c)$

   (c) If $p \mid (a^2 + b^2)$ and $p \mid (b^2 + c^2)$, then $p \mid (a^2 + c^2)$.

5. The square-free numbers are those integers k which are not divisible by the square of any prime (e.g. $1, 2, 3, 5, 6, 7, 10, 11, 13, \ldots$). Prove that every integer ≥ 2 is uniquely the product of a square and a square-free number.

6. Recall that $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for positive integers a, b.

   (a) In Example 2.25 we saw that the same formula *does not* necessarily hold when applied to *three* integers a, b, c. Find another such counter-example.

   (b) Is it ever true that $\gcd(a, b, c) \cdot \operatorname{lcm}(a, b, c) = abc$ for positive integers a, b, c? In general is the LHS less than or greater than abc? Make a hypothesis and try to prove it.

7. Suppose that g, m are positive integers. Prove that $g \mid m$ if and only if there exist integers a, b such that $\gcd(a, b) = g$ and $\operatorname{lcm}(a, b) = m$.