Chapter 6

Integer Operators

This chapter presents several computational problems for which integer algorithms based on number-theoretic principles are markedly faster than primitive algorithms tied more closely to the definitions.

6.1 EUCLIDEAN ALGORITHM

The *Euclidean algorithm* is a method for calculating the greatest common divisor of two integers. It is faster by far than the primitive method of successive trial divisors and methods based on factoring.

REVIEW FROM §3.1 AND APPENDIX A2:

- Let n and d be integers. If $\exists q \in \mathbb{Z}$ such that $n = dq$, then we say that d ***divides*** n, and we write $d \setminus n$.
- A ***prime number*** is a positive integer $p > 1$ such that p has no divisors except 1 and itself.
- Let m and n be integers whose greatest common divisor is 1. Then we say that m and n are ***relatively prime***. Notation $m \perp n$.
- The ***Fundamental Theorem of Arithmetic***: every positive integer n has a unique representation as a product of powers of ascending primes.

  $$n \;=\; p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

  (The number 1 is the empty product.)

Successive Trial-Divisors Algorithm

A primitive algorithm for calculating $\gcd(m, n)$ considers trial divisors in ascending order. Algorithm 6.1.1 considers trial divisors in decreasing order, thereby terminating the first time it finds a common divisor, so it runs relatively faster than the ascending version whenever $\gcd(m, n) > 1$. Worst-case time remains $\Theta(m)$.

Algorithm 6.1.1: Near-Primitive GCD Method

```
Input: non-negative integers $m$, $n$, not both 0
Output: $\gcd(m,\ n)$
Function $GCD1\,(m,\ n)$
if $\min\{m,\ n\} = 0$ then return $\max\{m,\ n\}$;
for $d := \min\{m,\ n\}$ to 1 step $-1$
    if $d \backslash m$ and $d \backslash n$ then return $d$;
    continue
```

The following minor modification of Algo 6.1.1 considers only the possible divisors $d = \lfloor m/k \rfloor$ for $k = 1, \ldots, \lfloor \sqrt{m} \rfloor$. This decreases the worst-case time to $\lfloor \sqrt{m} \rfloor$.

Algorithm 6.1.2: Elementary GCD Method

```
Input: integers $m$, $n$, with $0 \leq m \leq n$ and $0 \neq n$
Output: $\gcd(m,\ n)$
Function $GCD2\,(m,\ n)$
if $m = 0$ then return $n$;
for $k := 1$ to $\lfloor \sqrt{m} \rfloor$
    $d := \lfloor m/k \rfloor$;
    if $d \backslash m$ and $d \backslash n$ then return $d$;
    continue
```

Prime-Decomposition Method

A different method for calculating the greatest common divisor of the numbers m and n, and their least common multiple as well, is commonly taught in an early school grade. It starts with a factorization of m and n into primes.

$$\begin{aligned} m &= 2^{d_2} \cdot 3^{d_3} \cdot 5^{d_5} \cdot \cdots \\ n &= 2^{e_2} \cdot 3^{e_3} \cdot 5^{e_5} \cdot \cdots \end{aligned}$$

It then applies the rule

$$\gcd(m,\ n) = 2^{\min\{d_2,e_2\}} \cdot 3^{\min\{d_3,e_3\}} \cdot 5^{\min\{d_5,e_5\}} \cdot \cdots \quad (6.1:1)$$

$$\operatorname{lcm}(m,\ n) = 2^{\max\{d_2,e_2\}} \cdot 3^{\max\{d_3,e_3\}} \cdot 5^{\max\{d_5,e_5\}} \cdot \cdots \quad (6.1:2)$$

Example 6.1.1: Here are two prime-power factorizations.

$$\begin{aligned} 720 &= 2^4 \cdot 3^2 \cdot 5 \\ 168 &= 2^3 \cdot 3 \cdot 7 \end{aligned}$$

We now apply the elementary school method.

$$\begin{aligned} \gcd(720,\ 168) &= 2^{\min\{4,3\}} \cdot 3^{\min\{2,1\}} \cdot 5^{\min\{1,0\}} \cdot 7^{\min\{0,1\}} \\ &= 2^3 \cdot 3 \ = \ 24 \\ \operatorname{lcm}(720,\ 168) &= 2^{\max\{4,3\}} \cdot 3^{\max\{2,1\}} \cdot 5^{\max\{1,0\}} \cdot 7^{\max\{0,1\}} \\ &= 2^4 \cdot 3^2 \cdot 5 \cdot 7 \ = \ 5040 \end{aligned}$$

When this method is taught at lower school levels, the presumption is that the user *already knows the prime factorizations* of the two numbers. If neither is known, it may take some effort to calculate the prime factors. The following example illustrates what happens when this is not the case.

Example 6.1.2: Hand-calculator evaluation of

$$\gcd(6469901,\ 11503649)$$

by prime power factorizations is daunting, because those factorizations are not immediately at hand, and they must be calculated to proceed with the easier step. This greatest common divisor is evaluated quickly by the Euclidean algorithm, as will be shown presently.

Quotient and Mod Functions

Some basic concepts from integer division are used in the Euclidean algorithm.

DEF: The ***integer quotient*** of dividing an integer $n \geq 0$ by an integer $d > 0$ is defined recursively (in effect, by repeated subtraction)

$$\text{quotient}(n,\ d) \;=\; \begin{cases} 0 & \text{if } n < d \\ 1 + \text{quotient}(n-d,\ d) & \text{otherwise} \end{cases}$$

Remark: Equivalently, for $n \geq 0$ and $d > 0$,

$$\text{quotient}(n,\ d) \;=\; \left\lfloor \frac{n}{d} \right\rfloor$$

DEF: The ***remainder (or residue)*** of dividing an integer $n \geq 0$ by an integer $d > 0$ is the number

$$n \bmod d \;=\; n \;-\; \text{quotient}\,(n,\; d) \cdot d$$

The associated binary operation is called the ***mod function***, as previously noted in §1.1.

Example 6.1.1, cont.: For 720 as dividend and 168 as divisor, we have

$$\text{quotient}\,(720,\; 168) \;=\; \left\lfloor \frac{720}{168} \right\rfloor \;=\; 4$$

and

$$\begin{aligned} 720 \bmod 168 \;&=\; 720 \;-\; 4 \cdot 168 \\ &=\; 720 \;-\; 672 \\ &=\; 48 \end{aligned}$$

Prop 6.1.1. *The integer pairs* $\{m,\; n\}$ *and* $\{m,\; n + km\}$ *have the same set of common divisors, for every integer* k.

Proof: Let d be any common divisor of m and n, say $m = rd$ and $n = sd$. Then

$$m + kn \;=\; rd \;+\; ksd \;=\; (r + ks)\,d$$

Thus, the number d divides $m + kn$. In the opposite direction, if $m = rd$ and $n + km = td$, then

$$n \;=\; td \;-\; krd \;=\; (t - kr)\,d \qquad\qquad \diamondsuit$$

Corollary 6.1.2. *For every pair of integers m and n such that $0 < m \leq n$,*

$$\gcd(n,\ m) \ = \ \gcd(m,\ n \bmod m)$$

Proof: Suppose that $q = \text{quotient}(n,\ m)$. Then

$$\begin{aligned} \gcd(n,\ m) &= \gcd(m,\ n - qm) && \text{(by Prop 6.1.1)} \\ &= \gcd(m,\ n \bmod m) && \diamondsuit \end{aligned}$$

The strategy of the ***Euclidean algorithm*** is to apply Corollary 6.1.2 recursively. The following version captures this idea.

Algorithm 6.1.3: Recursive Euclidean Algorithm

```
Input: integers $n, m \geq 0$, not both 0
Output: $\gcd(n,\ m)$
 Recursive Function $\gcd(n,\ m)$
 If $n = 0$ then return $m$;
 If $m = 0$ then return $n$;
   else return $\gcd(m,\ n \bmod m)$
```

Example 6.1.1, cont.: This easy calculation illustrates the method.

$$\begin{aligned} \gcd(720,\ 168) &= \gcd(168,\ 48) \\ &= \gcd(48,\ 24) \\ &= \gcd(24,\ 0) \\ &= 24 \end{aligned}$$

Example 6.1.2, cont.: Here the calculations are mildly tedious, yet easier than trying to factor the two numbers.

$$\begin{aligned}
\gcd(11503649,\ 6469901) &= \gcd(6469901,\ 5033748)\\
&= \gcd(5033748,\ 1436153)\\
&= \gcd(1436153,\ 725289)\\
&= \gcd(725289,\ 710864)\\
&= \gcd(710864,\ 14425)\\
&= \gcd(14425,\ 4039)\\
&= \gcd(4039,\ 2308)\\
&= \gcd(2308,\ 1731)\\
&= \gcd(1731,\ 577)\\
&= \gcd(577,\ 0)\\
&= 577
\end{aligned}$$

Prop 6.1.3. *Given two numbers n and m, with $n \geq m$, let f_r be the smallest Fibonacci number that exceeds n. Then the number of recursive calls in the Euclidean algorithm is at most r.*

Proof: Suppose that there are s calls. Then let

$$n_0, n_1, \ldots, n_s$$

be the sequence of values of the first argument in the successive calls. Thus,

$$n_0 = n \quad \text{and} \quad n_s = \gcd(n, m)$$

We observe that $n_s \geq 1 > f_0$ and that $n_{s-1} \geq 2 > f_1$. It follows by induction, in general, that

$$n_{s-k-2} \; > \; f_{k+2} \; = \; f_{k+1} + f_k$$

because

$$n_{s-k-2} \; \geq \; n_{s-k-1} + n_{s-k} \; > \; f_{k+1} + f_k$$

In particular, $n_0 > f_s$. Therefore, $s < r$. ♢

Remark: Intuitively, the number of recursive calls is at its largest, relative to the size of the numbers supplied as input, when the input supplied is two consecutive Fibonacci numbers, since then all the quotients are 1, each remainder is the next lower Fibonacci number, and the numbers passed in the recursion are reduced as little as possible at each step. Since the growth of the Fibonacci sequence is exponential, as we proved in §2.5, we conclude that in this computationally "worst case", the number of recursive calls is proportional to the logarithm of the size of the input.

Extended Euclidean Algorithm

Keeping track of the quotients and remainders at each division step of the Euclidean algorithm is useful in extending its capability. In the Euclidean computation of gcd (n, m), define

$$m_0 \; = \; m \qquad \text{and} \quad n_0 \; = \; n \tag{6.1.3}$$

and then, if after $j-1$ steps the recursion continues, define

$$\begin{aligned} q_{j-1} &= \left\lfloor \frac{n_{j-1}}{m_{j-1}} \right\rfloor \\ n_j &= m_{j-1} \qquad (6.1.4) \\ m_j &= n_{j-1} - q_{j-1} m_{j-1} \qquad (6.1.5) \end{aligned}$$

Numerous applications involve the following result.

Thm 6.1.4. *For every pair of non-negative integers m and n, not both 0, there are numbers N and M such that*

$$\gcd(n,\ m) \ = \ Nn + Mm$$

Proof: Suppose that the recursion of the Euclidean algo stops at the k^{th} call, so that $m_k = 0$ and $n_k = \gcd(n, m)$. Then, if we define $N_k = 1$ and $M_k = 0$, we have

$$N_k n_k + M_k m_k \ = \ 1n_k + 0m_k \ = \ \gcd(n, m)$$

It follows from (6.1.4) and (6.1.5) that

$$\begin{aligned} \gcd(n,\ m) &= N_k(m_{k-1}) + M_k(n_{k-1} - q_{k-1}m_{k-1}) \\ &= M_k n_{k-1} + (N_k - M_k q_{k-1}) m_{k-1} \end{aligned}$$

Whenever $k \geq j > 0$, we inductively define (with decreasing j)

$$\begin{aligned} N_{j-1} &= M_j \\ M_{j-1} &= N_j - M_j q_{j-1} \end{aligned}$$

and, thus,

$$\gcd(n,\ m) \;=\; N_{j-1}n_{j-1} + M_{j-1}m_{j-1} \quad \text{for } k \geq j \geq 0$$

In particular,

$$\begin{aligned} \gcd(n,\ m) &= N_0 n_0 + M_0 m_0 \\ &= N_0 n + M_0 m \qquad \text{by (6.1.3)} \qquad \diamondsuit \end{aligned}$$

DEF: The ***extended Euclidean algorithm*** includes the computation of N and M s.t. $Nn + Mm = \gcd(n, m)$, as in Theorem 6.1.4.

Example 6.1.1, cont.: When preparing to apply the extension of the Euclidean algorithm, the steps of the calculation of the greatest common divisor are arranged in tabular form.

j	n_j	m_j	q_j
0	720	168	4
1	168	48	3
2	48	24	2
3	24	0	*STOP*

To continue with the extension, start by regarding the next-to-bottom row as the *current row.* Let j be its row number, in this case row 2. In that next-to-bottom row, write

$$1 \cdot n_j \,+\, 0 \cdot m_j \;=\; 1 \cdot (n_{j-1} - q_{j-1}m_{j-1})$$

with appropriate values substituted for every subscripted variable. In this case, the substitution yields the equation

$$1 \cdot 24 + 0 \cdot 0 \;=\; 1 \cdot (168 - 3 \cdot 48)$$

which expresses the greatest common divisor as a linear combination of n_j and m_j on the left and in terms of n_{j-1} and m_{j-1} on the right, which is then simplified into a standard form of linear combination, in this case

$$1 \cdot 168 \;-\; 3 \cdot 48$$

In general, working upwards, for each row of a by-hand calculation, the substitution of $n_{j-1} - q_{j-1}m_{j-1}$ for m_j uses values from the preceding row. There is an implicit substitution of the value of m_{j-1} for the value of n_j, but since $m_{j-1} = n_j$, this does not require work. Continue upward until row 0 is reached, at which point the greatest common divisor is expressed as a linear combination of n_0 and m_0, thereby completing the objective of the extended algorithm.

j	n_j	m_j	q_j	
0	720	168	4	$(-3) \cdot 720 + 13 \cdot 168$
1	168	48	3	$1 \cdot 168 - 3 \cdot 48 = 1 \cdot 168 - 3 \cdot (720 - 4 \cdot 168)$
2	48	24	2	$1 \cdot 24 + 0 \cdot 0 \;=\; 1 \cdot (168 - 3 \cdot 48)$
3	24	0	●	

In this case, we see that

$$(-3) \cdot 720 + 13 \cdot 168 \;=\; \gcd(720,\; 168) \;=\; 24$$

Thus, $N = -3$ and $M = 13$.

Corollary 6.1.5. *For every pair of non-negative integers m and n, not both 0, if $\hat{N}$ and $\hat{M}$ are numbers such that*

$$\gcd(n,\ m) \ = \ \hat{N}n + \hat{M}m$$

then $\hat{N}n + \hat{M}m$ is the smallest positively valued combination $Nn + Mm$ with integer multipliers N and M.

Proof: By Theorem 6.1.4, $\gcd(n,\ m)$ equals some combination $Nn+Mm$. Since $\hat{N}n+\hat{M}m$ is the smallest combination of n and m, it follows that

$$\hat{N}n + \hat{M}m \ \leq \ \gcd(n, m)$$

Since $\gcd(m,n) \setminus n$ and $\gcd(m,n) \setminus m$, it follows that for every choice of integers N and M, we have

$$\gcd(m,\ n) \setminus Nn + Mm$$

In particular,

$$\gcd(m,\ n) \setminus \hat{N}n + \hat{M}m$$

It follows that $\gcd(m,n) \leq \hat{N}n + \hat{M}m$. $\diamondsuit$

The GCD of Two Fibonacci Numbers

We conclude this section by combining what we know about Fibonacci numbers with what we know about greatest common divisors to produce the fascinating result that $\gcd(f_n, f_m) = f_{\gcd(n,m)}$. Some review and preliminary propositions are helpful.

REVIEW FROM §2.6:

- Thm 2.6.1 [Forward-Shift Identity]. The Fibonacci numbers satisfy the equation

$$f_{n+k} = f_k f_{n+1} + f_{k-1} f_n \qquad \text{for all } k \geq 1$$

- Cor 2.6.2. For all $k \geq 0$, the Fibonacci number f_{kn} is a multiple of the Fibonacci number f_n.

Prop 6.1.6. *Let m, n, and r be integers such that $r \perp m$. Then*

$$\gcd(rn, m) = \gcd(n, m)$$

Proof: Since any divisor of both m and n is also a divisor of m and rn, it follows that $\gcd(n, m) \leq \gcd(rn, m)$. Now suppose that $Nn + Mm = \gcd(n, m)$ and that $Cr + Dm = 1$. It follows that $NCr + NDm = N$ and, thus, that

$$\begin{aligned} \gcd(n, m) &= (NCr + NDm)n + Mm \\ &= NCrn + NDmn + Mm \\ &= (NC)rn + (NDn + M)m \end{aligned}$$

Since $\gcd(rn, m)$ is the smallest combination of rn and m, it follows that

$$\gcd(rn, m) \leq \gcd(n, m) \qquad \diamondsuit$$

Proposition 6.1.7. *For $n \geq 1$, $\gcd(f_n, f_{n-1}) = 1$.*

Proof: Calculation of $\gcd(f_n, f_{n-1})$ by the Euclidean algorithm terminates with a value of 1. $\diamondsuit$

Cor 6.1.8. *For $n \geq 1$ and $k \perp n$, $\gcd(f_{kn+1}, f_n) = 1$.*

Proof: By Corollary 2.6.2, f_n divides f_{kn}. Therefore,

$$\begin{aligned} \gcd(f_n, f_{kn+1}) &= \gcd(f_{kn}, f_{kn+1}) && \text{(Prop 6.1.6)} \\ &= 1 && \text{(Prop 6.1.7)} \quad \diamondsuit \end{aligned}$$

And now for the punch line.

Thm 6.1.9. *For $n \geq 0$ and $m \geq 1$,*

$$\gcd(f_n, f_m) = f_{\gcd(n,m)}$$

Proof: Suppose that $n = qm + r$, where $0 \leq r < m$. Then

$$\begin{aligned} &\gcd(f_n,\, f_m) = \gcd(f_{qm+r},\, f_m) \\ &= \gcd(f_{qm+1} f_r + f_{qm} f_{r-1},\, f_m) && \text{(Thm 2.6.1)} \\ &= \gcd(f_{qm+1} f_r,\, f_m) && \text{(Cor 2.6.2 and Prop 6.1.1)} \\ &= \gcd(f_r,\, f_m) && \text{(Cor 6.1.8 and Prop 6.1.6)} \quad \diamondsuit \end{aligned}$$

6.2 CHINESE REMAINDER THM

The extended Euclidean algorithm has many applications, including the solution of a system of *linear congruences.* The existence of solutions to certain systems is ensured by the *Chinese remainder theorem.*

Congruence Modulo m

DEF: A ***congruence modulo*** m is a relational statement of the form

$$a \equiv b \text{ (modulo } m)$$

It means that $m \setminus b - a$. (We sometimes omit parens.)

Example 6.2.1:

$$17 \equiv 2 \text{ (modulo 5) and } -8 \equiv 2 \text{ (modulo 5)}$$

The relation called congruence *modulo m* and the operator called *mod* have a similarity in their names. Their mathematical connection is as follows.

Proposition 6.2.1. *Let a and b be any integers and m a positive integer. Then*

$$a \equiv b \text{ (modulo } m)$$

if and only if

$$a \bmod m = b \bmod m$$

Proof: Suppose that $a = qm+r$ and $b = q'm+r'$ with $0 \leq r, r' < m$, so that $a \bmod m = r$ and $b \bmod m = r'$. We observe that the assertion $a \equiv b$ (modulo m) simply means $m \setminus b - a$, which is equivalent to the relation

$$m \setminus (q'm + r') - (qm + r)$$

which is equivalent, in turn, to the relation

$$m \setminus r' - r$$

Since $|r' - r| < m$, this holds if and only if $r' = r$, and, accordingly, if and only if $a \bmod m = b \bmod m$. ♢

Linear Congruence Modulo m

Like a system of linear equations, a *system of linear congruences* may possibly have a solution.

DEF: For integers a, b, and $m > 0$, a ***linear congruence*** is a relation of the form

$$ax \equiv b \text{ (modulo } m)$$

DEF: For positive moduli $m_1, m_2, \ldots, m_k$, a ***system of linear congruences*** is a list

$$\begin{aligned} a_1x &\equiv b_1 \text{ (modulo } m_1) \\ a_2x &\equiv b_2 \text{ (modulo } m_2) \\ &\vdots \\ a_kx &\equiv b_k \text{ (modulo } m_k) \end{aligned}$$

A ***solution to the system of congruences*** is an integer x that satisfies all of them.

Example 6.2.2: Consider the system of congruences

$$\begin{aligned} x &\equiv 2 \text{ (modulo 3)} \\ x &\equiv 3 \text{ (modulo 5)} \\ x &\equiv 1 \text{ (modulo 7)} \end{aligned}$$

We observe that $x = 8$ is a solution.

A Lemma on Relatively Prime Numbers

The Chinese remainder theorem yields a sufficient condition for a system of linear congruences to have an essentially unique solution. Moreover, there is a systematic way to find solutions. The following proposition serves as a lemma in the proof of the Chinese remainder theorem.

Prop 6.2.2. *Let m and n be relatively prime, and let Q be an integer such that $m \setminus Q$ and $n \setminus Q$. Then $mn \setminus Q$.*

Proof: Suppose that $Q = mr$ and $Q = ns$. Since $m \perp n$, there are integers N and M such that $Nn + Mm = 1$, by Theorem 6.1.4. Thus,

$$\begin{aligned} Q &= QNn + QMm \\ &= mrNn + nsMm \\ &= mn(rN + sM) \end{aligned} \qquad \diamondsuit$$

Remark: An alternative proof of Proposition 6.2.2 requires prior proof of the uniqueness of the factorization into prime powers, which is a substantially longer proof than the proof above.

Encoding by Residues

Some aspects of number theory are quite ancient. What is now described dates back to the Chinese mathematician Sun Tsŭ in the 4^{th} century C.E.

DEF: A set of positive integers $\{m_1, \ldots, m_k\}$ is a ***system of independent moduli*** if $m_i \perp m_j$ whenever $i \neq j$.

DEF: The ***tuple of residues*** of an integer n with respect to a system $\{m_1, \ldots, m_k\}$ of independent moduli is the k-tuple

$$(n \bmod m_1, \ldots, n \bmod m_k)$$

The following table shows the tuple of residues of the numbers 0 to 20 with respect to the mutually independent moduli 3, 4, and 5.

Table 6.2.1 Residues modulo 3, 4, and 5.

n	n mod 3	n mod 4	n mod 5
0	0	0	0
1	1	1	1
2	2	2	2
3	0	3	3
4	1	0	4
5	2	1	0
6	0	2	1
7	1	3	2
8	2	0	3
9	0	1	4
10	1	2	0
11	2	3	1
12	0	0	2
13	1	1	3
14	2	2	4
15	0	3	0
16	1	0	1
17	2	1	2
18	0	2	3
19	1	3	4
20	2	0	0

No two of the rows have the same list of residues, and there would be no repetition of rows until after the 60th row. This observation was generalized by Sun Tsŭ, as now indicated.

Theorem 6.2.3 [*Chinese Remainder Theorem*]. *Let $\{m_1, \ldots, m_k\}$ be a system of independent moduli, with $M = m_1 m_2 \cdots m_k$. Then the mapping*

$$n \;\mapsto\; (n \bmod m_1, \ldots, n \bmod m_k)$$

from the integer interval $[0 : M - 1]$ to the set of possible tuples of residues with respect to $\{m_1, \ldots, m_k\}$ is a one-to-one and onto mapping.

Proof: Since the domain $[0 : M - 1]$ and the codomain of tuples of residues with respect to $\{m_1, \ldots, m_k\}$ have the same cardinality M, it is sufficient, by the pigeonhole principle (see §0.3), to prove that no two numbers in $[0 : M - 1]$ have the same set of residues.

Suppose, to the contrary, that $0 \leq b < c < M$ and that

$$c \bmod m_j \;=\; b \bmod m_j \quad \text{for } j = 1, \ldots, k$$

Then

$$m_j \setminus (c - b) \quad \text{for } j = 1, \ldots, k$$

Accordingly, iterative application of Prop 6.2.2 would imply that

$$m_1 m_2 \cdots m_k \setminus (c - b) \quad \text{for } j = 1, \ldots, k$$

It would follow that $M \setminus (c - b)$, since $M = m_1 m_2 \cdots m_k$. But then $c - b \geq M$, which contradicts the prior supposition that $0 \leq b < c < M$. ♢

Arithmetic on Residue Tuples

Much of the value of encoding numbers by residues is that arithmetic operations on the residues produce the residues of the result of the operations directly on the numbers.

DEF: The ***sum of two k-tuples*** of residues with respect to a list of moduli $\{m_1, \ldots, m_k\}$ is the k-tuple whose j^{th} coordinate is the sum of the two j^{th} coordinates modulo m_j.

Example 6.2.3:

n	n mod 3	n mod 4	n mod 5
2	2	2	2
+ 8	2	0	3
= 10	1	2	0

DEF: The ***product of two k-tuples*** of residues with respect to a list of moduli $\{m_1, \ldots, m_k\}$ is the k-tuple whose j^{th} coordinate is the product of the two j^{th} coordinates modulo m_j.

Example 6.2.4:

n	n mod 3	n mod 4	n mod 5
2	2	2	2
× 8	2	0	3
= 16	1	0	1

Encoding by residues is that it respects arithmetic. That is, the sum of the tuples for numbers r and s is the tuple of the sum $r + s$, and the product of the tuples for numbers r and s is the tuple of the product rs.

Remark: The arithmetic-preservation property enables us to add and multiply small residues instead of large numbers. If there is a large amount of arithmetic, then the cost of encoding and subsequently decoding the result of the computations may be amortized.

Residue Decoding

The following theorem provides a method by which, knowing only the residues of a number, one could recover the number itself.

Theorem 6.2.4 [*Chinese Remainder Decoding*]. *Let m_1 and m_2 be positive integers and let Q_1 and Q_2 be integers such that*

$$Q_1 m_1 + Q_2 m_2 \;=\; 1$$

Let n be an integer such that $0 \leq n < m_1 m_2$, and such that

$$(n \bmod m_1,\, n \bmod m_2) \;=\; (r_1, r_2)$$

Then

$$r_1 Q_2 m_2 + r_2 Q_1 m_1 \;=\; n$$

Proof: Since $Q_1 m_1 + Q_2 m_2 = 1$, it follows that

$$m_2 \setminus Q_1 m_1 - 1 \quad \text{and} \quad m_1 \setminus Q_2 m_2 - 1$$

and, in turn, that

$$Q_1 m_1 \bmod m_2 \;=\; 1 \quad \text{and} \quad Q_2 m_2 \bmod m_1 \;=\; 1$$

Accordingly,

$$\begin{aligned} r_1 Q_2 m_2 \bmod m_1 &= r_1 \quad \text{and} \\ r_1 Q_2 m_2 + r_2 Q_1 m_1 \bmod m_1 &= r_1 \qquad (6.2.1) \end{aligned}$$

Similarly,

$$\begin{aligned} r_2 Q_1 m_1 \bmod m_2 &= r_2 \quad \text{and} \\ r_1 Q_2 m_2 + r_2 Q_1 m_1 \bmod m_2 &= r_2 \qquad (6.2.2) \end{aligned}$$

By the Chinese Remainder Theorem, there is only one number in the integer interval $[0 : m_1 m_2]$ whose residues modulo m_1 and modulo m_2 are r_1 and r_2, respectively. Thus,

$$r_1 Q_2 m_2 + r_2 Q_1 m_1 \;=\; n \qquad \diamondsuit$$

In combination with the extended Euclidean algorithm, Theorem 6.2.4 is used to decode any tuple of moduli. It is simplest for a 2-tuple, as now illustrated.

Example 6.2.5: Clearly, $8 \mapsto (2 \bmod 3,\, 3 \bmod 5)$. Either by simple observation or by an application of the extended Euclidean algorithm, we have

$$(-3) \cdot 3 + 2 \cdot 5 \;=\; 1 \;=\; Q_1 m_1 + Q_2 m_2$$

Chinese Remainder Decoding now recovers the encoded number 8.

$$\begin{aligned} r_1 Q_2 m_2 + r_2 Q_1 m_1 &= 2 \cdot 2 \cdot 5 + 3 \cdot (-3) \cdot 3 \\ &= 20 - 27 \;=\; -7 \\ &\equiv 8 \text{ (modulo 15)} \end{aligned}$$

Example 6.2.6: Decoding of the 2-tuple

$$(4 \bmod 8,\ 2 \bmod 9)$$

begins with determination of Q_1 and Q_2, easily in this case,

$$(-1) \cdot 8 + 1 \cdot 9 \ = \ 1 \ = \ Q_1 m_1 \ + \ Q_2 m_2$$

and finishes with the calculation

$$\begin{aligned} r_1 Q_2 m_2 \ + \ r_2 Q_1 m_1 \ &= \ 4 \cdot 1 \cdot 9 + 2 \cdot (-1) \cdot 8 \\ &= \ 36 \ - \ 16 \ = \ 20 \end{aligned}$$

Checking that $20 \mapsto (4 \bmod 8, 2 \bmod 9)$ confirms this decoding.

Decoding 3-Tuples and Larger Tuples

Decoding a k-tuple of residues with $k \geq 3$ involves iterative application of the following principle.

Proposition 6.2.5. *Suppose that m_1, m_2, and m_3 are mutually relatively prime. Then $m_1 m_2 \perp m_3$.*

Proof: If neither of the numbers m_1 nor m_2 has a prime divisor that occurs in the prime factorization of m_3, then $m_1 m_2$ has no prime divisor that occurs in the prime factorization of m_3, since the set of prime divisors of $m_1 m_2$ is the union of the set of prime divisors of m_1 and m_2. $\diamondsuit$

Example 6.2.7: Decoding of the 3-tuple

$$(4 \bmod 8,\ 2 \bmod 9,\ 3 \bmod 5)$$

begins with the calculation of Example 6.2.6 that

$$20 \mapsto (4 \bmod 8,\ 2 \bmod 9)$$

Any number n such that $n \equiv 20 \bmod 72$ satisfies both of the conditions $n \equiv 4 \bmod 8$ and $n \equiv 3 \bmod 5$. Subsequent decoding of the 2-tuple

$$(20 \bmod 72,\ 3 \bmod 5)$$

begins with finding multipliers Q_1 and Q_2 such that

$$Q_1 \cdot 72 + Q_2 \cdot 5 = 1$$

Either by "guessing" or by the extended Euclidean algorithm, we have

$$(-2) \cdot 72 + 29 \cdot 5 = 1$$

The calculation concludes with

$$\begin{aligned} r_1 Q_2 m_2 + r_2 Q_1 m_1 &= 20 \cdot 29 \cdot 5 + 3 \cdot (-2) \cdot 72 \\ &= 2900 - 432 = 2468 \\ &\equiv 308 \text{ (modulo 360)} \end{aligned}$$

Checking that

$$308 \mapsto (4 \bmod 8,\ 2 \bmod 9,\ 3 \bmod 5)$$

confirms this decoding.

6.3 POLYNOMIAL DIVISIBILITY

This section demonstrates how some of the integer operations of present interest are extendible to operations on polynomials. In particular, a pair of polynomials may have a greatest common divisor, there is a Euclidean algorithm for polynomials, and there are prime polynomials.

NOTATION: The degree of a polynomial $g(x)$ is denoted $\partial g(x)$.

DEF: A ***monic polynomial*** is a polynomial whose coefficient on the term of largest degree is 1.

Example 6.3.1: $x^4 + 5x^3 - 4x^2 + 7x + 14$ is a monic polynomial.

The Polynomial Ring over the Integers

NOTATION: The set of polynomials of finite degree in one indeterminate x, with integer coefficients, is denoted $\mathbb{Z}[x]$.

TERMINOLOGY: In view of its algebraic properties, $\mathbb{Z}[x]$ is called a ***polynomial ring*** (see Appendix A2).

Divisibility and Mod for Polynomials

Division of polynomials is a generalization of *long division*, with a *quotient* and a *remainder.* In effect, we subtract multiples of the divisor from the dividend, until what is left is of lower degree than the divisor.

DEF: The ***quotient of dividing a polynomial***

$$g(x) \;=\; g_r x^r + g_{r-1}x^{r-1} + \cdots + g_0$$

of degree r by a polynomial of degree s

$$h(x) \;=\; h_s x^s + h_{s-1}x^{s-1} + \cdots + h_0$$

is defined recursively (using repeated subtraction):
If $r < s$ then $\text{quotient}\,(g(x),\, h(x)) \;=\; 0$, and, otherwise, $\text{quotient}\,(g(x),\, h(x)) \;=$

$$\frac{g_r}{h_s}\,x^{r-s} + \text{quotient}\left(g(x) - \frac{g_r}{h_s}\,x^{r-s}h(x),\; h(x)\right)$$

DEF: The ***remainder of division of a polynomial***

$$g(x) \;=\; g_r x^r + g_{r-1}x^{r-1} + \cdots + g_0$$

by a non-zero polynomial

$$h(x) \;=\; h_s x^s + h_{s-1}x^{s-1} + \cdots + h_0$$

is the polynomial

$$g(x) \bmod h(x) \;=\; g(x) - \text{quotient}\,(g(x),\, h(x))\, h(x)$$

DEF: The non-zero polynomial $h(x)$ ***divides*** the polynomial $g(x)$ if there is a polynomial $f(x)$ such that

$$g(x) \;=\; h(x)f(x)$$

This relation is denoted $h(x) \setminus g(x)$.

Clearly, the polynomial $h(x)$ divides the polynomial $g(x)$ if and only if

$$g(x) \bmod h(x) \;=\; 0$$

Example 6.3.2: The polynomials x^3-x^2+1 and x^3-2 both divide the polynomial $x^6-x^5-x^3+2x^2-2$, since

$$(x^3-x^2+1)(x^3-2) \;=\; x^6-x^5-x^3+2x^2-2$$

Common Divisors of Polynomials

DEF: A ***common divisor*** of two or more polynomials is a polynomial that divides both or all of them.

The following proposition is analogous to Prop 6.1.1.

Prop 6.3.1. *Let $a(x)$, $b(x)$, and $c(x)$ be polynomials in the polynomial ring $\mathbb{Z}[x]$. Then the polynomial pairs $\{a(x), b(x)\}$ and $\{a(x),\ b(x)+a(x)c(x)\}$ have the exact same set of common divisors.*

Proof: Let $h(x)$ be any common divisor of $a(x)$ and $b(x)$, say $a(x) = u(x)h(x)$ and $b(x) = v(x)h(x)$. Then

$$\begin{aligned} a(x) \,+\, c(x)b(x) \;&=\; u(x)h(x) \,+\, c(x)v(x)h(x) \\ &=\; (u(x) \,+\, c(x)v(x))h(x) \end{aligned}$$

Conversely, if $a(x) = u(x)h(x)$ and $b(x) + a(x)c(x) = v(x)h(x)$, then

$$\begin{aligned} b(x) &= v(x)h(x) - a(x)c(x) \\ &= v(x)h(x) - u(x)h(x)c(x) \\ &= (v(x) - u(x)c(x))\, h(x) \end{aligned} \qquad \diamondsuit$$

DEF: A ***greatest common divisor of two polynomials***

$$\begin{aligned} a(x) &= a_r x^r + a_{r-1}x^{r-1} + \cdots + a_0 \quad \text{and} \\ b(x) &= b_s x^s + b_{s-1}x^{s-1} + \cdots + b_0 \end{aligned}$$

is a common divisor polynomial $g(x)$ of highest degree.

NOTATION: The notation $\gcd(g(x), h(x))$ often refers to the monic greatest common divisor of $g(x)$ and $h(x)$.

Example 6.3.3: The polynomial x^3-x^2+1 is a greatest common divisor of the polynomials $x^6 - x^5 - x^3 + 2x^2 - 2$ and $x^4 - x^2 + x + 1$. The polynomial $x^3 - x^2 + 1$ is monic, and we write

$$\begin{aligned} &\gcd\left(x^6 - x^5 - x^3 + 2x^2 - 2,\ \ x^4 - x^2 + x + 1\right) \\ &\quad = x^3 - x^2 + 1 \end{aligned}$$

Euclidean Algorithm for Polynomials

Thm 6.3.2 [***Euclidean Reduction for Polyns***]. *Let $g(x)$ and $h(x)$ be polyns such that $0 < \partial h(x) \leq \partial g(x)$. Then*

$$\gcd\left(h(x),\ g(x)\right) \ = \ \gcd\left(h(x),\ g(x) \bmod h(x)\right)$$

Proof: Suppose that $q(x) = \textit{quotient}\,(g(x), h(x))$. Then

$$\begin{aligned} \gcd\left(h(x),\ g(x)\right) &= \gcd\left(h(x),\ g(x) - q(x)h(x)\right) \quad \text{(Prop 6.3.1)} \\ &= \gcd\left(h(x),\ g(x) \bmod h(x)\right) \qquad \diamondsuit \end{aligned}$$

DEF: The ***Euclidean algorithm for polynomials*** is to iterate Euclidean reduction until a residue of zero is achieved.

Example 6.3.4: The process is directly analogous to the integer version.

$$\begin{aligned} &\gcd\left(x^5 - 1,\ x^3 - 3x^2 + 3x - 1\right) \\ &= \gcd\left(x^3 - 3x^2 + 3x - 1,\ 10x^2 - 15x + 5\right) \\ &= \gcd\left(10x^2 - 15x + 5,\ \frac{1}{4}x - \frac{1}{4}\right) \\ &= \gcd\left(\frac{1}{4}x - \frac{1}{4},\ 0\right) \\ &= x - 1 \end{aligned}$$

Remark: There is also an extended Euclidean algorithm for polynomials.

Prime Polynomials

DEF: A monic polynomial $g(x) \neq 1$ is a ***prime polynomial*** if it has no monic divisors of positive degree except for itself.

Example 6.3.5: Any linear polynomial $x + k$ is prime.

Example 6.3.6: A quadratic polynomial $x^2 + bx + c$ is prime over the integers, unless it has two integers (perhaps both the same) as its roots. For instance, $x^2 - 2$ is prime. More generally, by the quadratic equation, it follows that for the roots to be integers, it is a necessary condition that $b^2 - 4c$ must be the square of an integer.

6.4 PRIME & COMPOSITE MODULI

When evaluating a congruence, first expanding the moduland and then dividing by the modulus is slow. Number theory and algebra can make it faster.

FROM APPENDIX A2:

- The domain of the ring of ***integers modulo n***, denoted $\mathbb{Z}_n$, is the set of numbers
$$\{0, \quad 1, \quad \ldots, \quad n-1\}$$
- The binary operations of ***addition modulo n*** (+) and ***multiplication modulo n*** ($\cdot$) in the ring $\mathbb{Z}_n$ are given by the rules
$$\begin{aligned} b\,(\text{modulo } n) + c\,(\text{modulo } n) &= b + c\,(\text{modulo } n) \\ b\,(\text{modulo } n) \cdot c\,(\text{modulo } n) &= b \cdot c\,(\text{modulo } n) \end{aligned}$$
In other words, if adding or multiplying two numbers as usual for integers happens to exceed $n-1$, then divide by n and use the remainder as the result.
- The number 0 is the additive identity of $\mathbb{Z}_n$.
- The number 1 is the multiplicative identity of $\mathbb{Z}_n$.
- The number k has $n-k$ as its additive inverse in $\mathbb{Z}_n$.
- Some numbers have multiplicative inverses in $\mathbb{Z}_n$. For instance, 13 is the inverse of 7 in $\mathbb{Z}_{90}$, since
$$13 \cdot 7 \;=\; 91 \;\equiv\; 1\,(\text{modulo } 90)$$

Existence of Inverses Modulo m

The general objective here to find solutions to congruences of the form

$$mx \equiv 1 \text{ (modulo } n)$$

for arbitrary positive integers m and n.

Proposition 6.4.1. *Let m and n be positive integers. Then m (modulo n) has a multiplicative inverse if and only if $m \perp n$.*

Proof: First, suppose that $m \perp n$. By the extended Euclidean algorithm, there are integers N and M such that

$$Nn + Mm = 1$$

Thus,

$$Mm \equiv 1 \text{ (modulo } n)$$

which implies that M mod n is a multiplicative inverse of m mod n in $\mathbb{Z}_n$.

Conversely, if $Mm \equiv 1$ (modulo n), then

$$n \setminus (Mm - 1)$$

Thus, there is an integer N such that $Nn = Mm - 1$ which implies that

$$Mm - Nn = 1$$

from which it follows that $m \perp n$. ♢

Corollary 6.4.2. *Let p be a prime number. Then all the numbers* $1, \ldots, p-1$ *have inverses in* $\mathbb{Z}_p$.

Proof: Since p is prime, all the numbers $1, \ldots, p-1$ are relatively prime to p. $\diamondsuit$

Remark: When p is prime, $\mathbb{Z}_p$ is a ***field***. See App A2.

The following three examples all illustrate the conclusion of Proposition 6.4.1.

Example 6.4.1: In the ring $\mathbb{Z}_6$, the numbers 1 and 5 (both relatively prime to 6) are their own inverses, but the numbers 2, 3, and 4 have no multiplicative inverses.

Example 6.4.2: In the ring $\mathbb{Z}_7$, the numbers $1, \ldots, 6$ (all relatively prime to 7) all have multiplicative inverses, in accord with Corollary 6.4.2, respectively, 1, 4, 5, 2, 3, 6.

Example 6.4.3: In the ring $\mathbb{Z}_8$, the numbers 1, 3, 5, 7 (all relatively prime to 8) are their own inverses, but 2, 4, 6 (not relatively prime to 8) have no multiplicative inverses.

Calculating Inverses Modulo n

The proof of Prop 6.4.1 provides a method for calculating the inverse modulo n of a number m such that $m \perp n$.

Step 1. Find integers N and M such that $Nn+Mm = 1$, for instance, by the extended Euclidean algo.

Step 2. Then take M mod n as the multiplicative inverse of m (modulo n).

Example 6.4.4: Since $16 \perp 21$, the number 16 must have a mult inverse modulo 21. Either by inspection or by the extended Euclidean algo, it can be determined that

$$4 \cdot 16 \; - \; 3 \cdot 21 \; = \; 1$$

Thus, the multiplicative inverse of 16 (modulo 21) is 4.

Uniqueness of Inverse Modulo m

TERMINOLOGY: In Example 6.4.4, the number 4 is described as *the* inverse of 16 modulo 21, rather than *an* inverse. In fact, the number 25 is another multiplicative inverse of 16 modulo 21, since

$$25 \cdot 16 \; - \; 19 \cdot 21 \; = \; 1$$

However, it is proved below that a number n has at most one inverse modulo m in the range

$$1, \ldots, m-1$$

The definite article *the* is often applied to such an inverse.

Lemma 6.4.3. *Let n be an integer and m an integer that is relatively prime to n. Then the numbers*

$$m, \quad 2m, \quad \ldots, \quad (n-1)m$$

are mutually non-congruent modulo n, i.e., a permutation of the numbers

$$1, \quad 2, \quad \ldots, \quad n-1$$

Proof: Proposition 6.4.1 implies that m has a multiplicative inverse modulo n, that is, a number M such that

$$Mm \;=\; 1 \;+\; Nn$$

for some number N. Consider two numbers r and s such that $1 \leq r$, $s \leq n-1$. Suppose that

$$rm \;\equiv\; sm \text{ (modulo } n)$$

Then $rmM \equiv smM$ (modulo n). It follows that

$$r(1+Nn) \;\equiv\; s(1+Nn) \text{ (modulo } n)$$

and, in turn, that

$$r \;\equiv\; s \text{ (modulo } n) \qquad \diamondsuit$$

Cor 6.4.4. *Let m and n be relatively prime positive integers. Then there is exactly one inverse M of m* (modulo n) *such that $1 \leq M < n$.* $\diamondsuit$

Example 6.4.5: Consider the prime $p = 7$ and the number $m = 4$. Then the sequence

$$\Big\langle km \bmod p \;\Big|\; k = 1, \ldots, p-1 \Big\rangle$$

is exactly the sequence

$$\begin{array}{l} 1 \cdot 4 \;=\; 4, \quad 2 \cdot 4 \;=\; 8, \quad 3 \cdot 4 \;=\; 12, \\ \qquad\qquad 4 \cdot 4 \;=\; 16, \quad 5 \cdot 4 \;=\; 20, \quad 6 \cdot 4 \;=\; 24 \end{array}$$

which reduces, modulo 7, to the sequence

$$\begin{array}{lll} 1 \cdot 4 \;\equiv\; 4 \text{ (modulo } n), & 2 \cdot 4 \;\equiv\; 1 \text{ (modulo } n), & 3 \cdot 4 \;\equiv\; 5 \text{ (modulo } n), \\ 4 \cdot 4 \;\equiv\; 2 \text{ (modulo } n), & 5 \cdot 4 \;\equiv\; 6 \text{ (modulo } n), & 6 \cdot 4 \;\equiv\; 3 \text{ (modulo } n) \end{array}$$

Thus, the number 2 is the unique inverse of 4 (modulo 7) in the range 1, ..., 6.

Fermat's Theorem

We now turn to the problem of *modular exponentiation*, that is, of evaluating an expression involving an exponential modulo a number, such as

$$3124^{214} \text{ (modulo } 20)$$

This is less tedious than it at first appears, since there is no need to evaluate 3124^{214}. A first reduction is based on the following proposition.

Proposition 6.4.5. *For any integers m and $n \geq 1$,*

$$m^r \text{ (modulo } n) \;\equiv\; (m \bmod n)^r \text{ (modulo } n)$$

Proof: Suppose that $m = qn + (m \bmod n)$. Then

$$m^r \;=\; (qn + (m \bmod n))^r$$

In the expansion of the exponentiated binomial on the right, the only term that does not have n as a factor is $(m \bmod n)^r$. Hence,

$$m^r \text{ (modulo } n) \;\equiv\; (m \bmod n)^r \text{ (modulo } n) \qquad \diamondsuit$$

In particular,

$$3124^{214} \text{ (modulo } 20) \;\equiv\; 4^{214} \text{ (modulo } 20)$$

A further kind of simplification begins with the choice of a convenient power of the base number 4. For instance, choosing the exponent 3 produces the following reduction of the exponent and easy evaluation.

$$\begin{aligned}
& 4^3 &=& \; 64 \;\equiv\; 4 \text{ (modulo 20)} \\
\Rightarrow \quad & 4^{214} &=& \; (4^3)^{71} \cdot 4 \;\equiv\; 4^{71} \cdot 4 \;\equiv\; 4^{72} \text{ (modulo 20)} \\
& &\equiv& \; (4^3)^{24} \;\equiv\; 4^{24} \;\equiv\; (4^3)^8 \;\equiv\; 4^8 \text{ (modulo 20)} \\
& &\equiv& \; (4^3)^2 \cdot 4^2 \;\equiv\; 4^2 \cdot 4^2 \;\equiv\; 4^4 \text{ (modulo 20)} \\
& &\equiv& \; 4^3 \cdot 4 \;\equiv\; 4 \cdot 4 \;\equiv\; 16 \text{ (modulo 20)}
\end{aligned}$$

Alternatively, if we choose the exponent 5,

$$\begin{aligned}
& 4^5 &=& \; 1024 \;\equiv\; 4 \text{ (modulo 20)} \\
\Rightarrow \quad & 4^{214} &=& \; (4^5)^{42} \cdot 4^4 \;\equiv\; 4^{42} \cdot 4^4 \;\equiv\; 4^{46} \;\equiv\; (4^5)^9 \cdot 4 \text{ (modulo 20)} \\
& &\equiv& \; 4^9 \cdot 4 \;\equiv\; 4^{10} \;\equiv\; (4^5)^2 \;\equiv\; 4^2 \;\equiv\; 16 \text{ (modulo 20)}
\end{aligned}$$

A theorem of Fermat permits such a calculation to go even more rapidly, when the modulus is prime. Its traditional name is *Fermat's Little Theorem.*

Theorem 6.4.6 [*Fermat's Little Theorem*]. *Let p be a prime number and let b be any integer that is not divisible by p. Then*

$$b^{p-1} \;\equiv\; 1 \text{ (modulo } p)$$

Proof: Lemma 6.4.3 implies that

$$\prod_{j=1}^{p-1} (jb) \;\equiv\; \prod_{j=1}^{p-1} j \;\equiv\; (p-1)! \text{ (modulo } p) \qquad (6.4.1)$$

Since multiplication modulo p retains commutativity,

$$\prod_{j=1}^{p-1}(jb) \equiv \left(\prod_{j=1}^{p-1} b\right) \prod_{j=1}^{p-1} j \text{ (modulo } p) \tag{6.4.2}$$

Combining (6.4.1) and (6.4.2) yields

$$b^{p-1}(p-1)! \equiv (p-1)! \text{ (modulo } p) \tag{6.4.3}$$

Applying Corollary 6.4.2 to all the factors of $(p-1)!$ in the congruence (6.4.3) implies the result

$$b^{p-1} \equiv 1 \text{ (modulo } p) \qquad \diamondsuit$$

Example 6.4.6: All the numbers

$$1^4 = 1,\ 2^4 = 16,\ 3^4 = 81,\ 4^4 = 256$$

are congruent to 1 modulo 5.

Example 6.4.7: Fermat's congruence cannot be used when the modulus is not prime. For instance,

$$\begin{aligned} 2^{11} &= 2048 \equiv 8 \text{ (modulo } 12) \\ 3^{11} &= 177147 \equiv 3 \text{ (modulo } 12) \end{aligned}$$

Remark: In §6.5, there is a generalization by Euler of Fermat's Little Theorem.

Wilson's Theorem

There is still more to be harvested from Corollary 6.4.2, the principle that the numbers $1, \ldots, p-1$ all have multiplicative inverses modulo a prime p.

Prop 6.4.7. *Let p be a prime number and let n be an integer that is not divisible by p. Then $n^2 \equiv 1$ (modulo p) if and only if $n \equiv \pm 1$ (modulo p).*

Proof: Suppose first that $n \equiv \pm 1$ (modulo p). That is, there is an integer k such that $n = kp \pm 1$. Then either

$$n^2 = (kp+1)^2 = k^2p^2 + 2kp + 1 \equiv 1 \text{ (modulo } p)$$

or

$$n^2 = (kp-1)^2 = k^2p^2 - 2kp + 1 \equiv 1 \text{ (modulo } p)$$

Conversely, suppose that $n^2 \equiv 1$ (modulo p). Then $p \setminus n^2 - 1$. It follows that

$$p \setminus (n-1)(n+1)$$

Thus, since p is prime, either $p \setminus n-1$ or $p \setminus n+1$. If $p \setminus n-1$, then $n \equiv 1$ (modulo p). If $p \setminus n+1$, then $n \equiv -1$ (modulo p). ♢

Cor 6.4.8. *Let p be prime. Then $(p-2)! \equiv 1$ (modulo p).*

Proof: Let $r \in \{2, \ldots, p-2\}$. By Prop 6.4.7, the number r cannot be its own multiplicative inverse modulo p, and that inverse must lie in that same range $\{2, \ldots, p-2\}$. It follows that the numbers $2, \ldots, p-2$ can be paired into inverses modulo p. Accordingly,

$$\prod_{j=2}^{p-2} j \equiv 1 \text{ (modulo } p)$$

Thus, $(p-2)! \equiv 1$ (modulo p). ♢

Theorem 6.4.9 [*Wilson's Theorem*]. *The congruence*

$$(m-1)! \equiv -1 \text{ (modulo } m)$$

holds if and only if m is prime.

Proof: If m is prime, then the congruence

$$(m-1)! \equiv -1 \text{ (modulo } m)$$

follows immediately from Corollary 6.4.8.

Conversely, if m is not prime, then m has a factor r such that $r \leq \lfloor\sqrt{m}\rfloor$, say $rs = m$. If $r < s$, then

$$\begin{aligned}(m-1)! &= rs \cdot \left(\prod_{j=1}^{r-1} j\right)\left(\prod_{j=r+1}^{s-1} j\right)\left(\prod_{j=s+1}^{m-1} j\right)\\ &\equiv 0 \cdot \left(\prod_{j=1}^{r-1} j\right)\left(\prod_{j=r+1}^{s-1} j\right)\left(\prod_{j=s+1}^{m-1} j\right) \equiv 0 \not\equiv -1 \text{ (modulo } m)\end{aligned}$$

If $r^2 = m = 4$, then

$$(m-1)! \;=\; 3! \;=\; 6 \;\not\equiv\; -1 \text{ (modulo 4)}$$

Otherwise, i.e., for $m \geq 6$, we have $\sqrt{m} > 2$, which implies that $2r < m$. Thus,

$$\begin{aligned}
(m-1)! &= r \cdot 2r \cdot \left(\prod_{j=1}^{r-1} j\right)\left(\prod_{j=r+1}^{2r-1} j\right)\left(\prod_{j=2r+1}^{m-1} j\right)\\
&\equiv 2 \cdot r^2 \cdot \left(\prod_{j=1}^{r-1} j\right)\left(\prod_{j=r+1}^{2r-1} j\right)\left(\prod_{j=2r+1}^{m-1} j\right)\\
&\equiv 2 \cdot 0 \cdot \left(\prod_{j=1}^{r-1} j\right)\left(\prod_{j=r+1}^{2r-1} j\right)\left(\prod_{j=2r+1}^{m-1} j\right)\\
&\qquad\qquad \text{(since } r^2 = m \equiv 0 \text{ (modulo } m))\\
&\equiv 0 \text{ (modulo } m) \qquad \diamondsuit
\end{aligned}$$

Remark: We have proved a sharpened version of Wilson's theorem, with values for $(m-1)!$ (modulo m) in all cases.

Quadratic Residues

DEF: The integer a is a ***quadratic residue*** of the integer m if $a \perp m$ and if the congruence

$$x^2 \;\equiv\; a \text{ (modulo } m)$$

has a solution. If the congruence $x^2 \equiv a \bmod m$ has no solution, then a is called a ***quadratic non-residue*** of m.

Remark: If c and d are congruent, then

$$c^2 \equiv d^2 \text{ (modulo } m)$$

Thus, the set of numbers c^2 such that $1 \leq c \leq m-1$ and $c \perp m$ is a complete set of quadratic residues of m.

Example 6.4.8: According to the remark above, the set

$$\begin{aligned} \{\, 1 \equiv 1^2, \quad 4 \equiv 2^2, \quad 2 \equiv 3^2, \quad 2 \equiv 4^2, \quad 4 \equiv 5^2, \quad 1 \equiv 6^2 \,\} \\ = \{1, \quad 2, \quad 4\} \end{aligned}$$

is the set of quadratic residues of 7. The numbers 3, 5, and 6 are quadratic non-residues of 7.

Example 6.4.9: The quadratic residues of 11 are

$$\begin{gathered} 1 \equiv 1^2 \equiv 10^2, \quad 4 \equiv 2^2 \equiv 9^2, \quad 9 \equiv 3^2 \equiv 8^2, \quad 5 \equiv 4^2 \equiv 7^2, \\ \text{and} \quad 3 \equiv 5^2 \equiv 6^2 \end{gathered}$$

The numbers 2, 6, 7, 8, and 10 are quadratic non-residues of 11.

Example 6.4.10: The quadratic residues of 15 are

$$1 \equiv 1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \quad \text{and} \quad 4 \equiv 2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2$$

Finding Solutions to a Quadratic

We now generalize some of the properties that may have been observed in these examples.

POWER OF ODD PRIME AS MODULUS

Theorem 6.4.10. *Let p be an odd prime, let n be a positive integer, and let a be an integer not divisible by p. Then the congruence*

$$x^2 \;\equiv\; a\,(\text{modulo } p^n) \tag{6.4.4}$$

has either two distinct solutions in the range $1, \ldots, p^n - 1$ *or no solutions at all.*

Proof: Suppose that b lies in the range $1, \ldots, p^n - 1$ and that

$$b^2 \equiv a \bmod p^n \tag{6.4.5}$$

Observe that $p^n - b$ lies in the range $1, \ldots, p^n - 1$, and that it is not equal to b, since p^n is odd. The calculation

$$\begin{aligned}(p^n - b)^2 &= p^{2n} - 2bp^n + b^2 \\ &\equiv b^2\,(\text{modulo } p^n)\end{aligned}$$

establishes that $p^n - b$ is a second solution to the congruence (6.4.4).

To see that there are no more than these two solutions, consider another putative solution, i.e., a number c such that

$$c^2 \;\equiv\; a\,(\text{modulo } p^n) \tag{6.4.6}$$

Congruences (6.4.5) and (6.4.6) together imply that

$$b^2 - c^2 \equiv 0 \text{ (modulo } p^n)$$

from which it follows that $p^n \setminus b^2 - c^2$, and, equivalently, that

$$p^n \setminus (b-c)(b+c)$$

Thus, either

$$p \setminus b - c \quad \text{or} \quad p \setminus b + c$$

If p were to divide both $b-c$ and $b+c$, then p would divide their sum $2b$. Yet, since p is an odd prime, it cannot divide 2, so it would necessarily divide b, implying that it divides a, which would contradict the choice of the number a. Accordingly, the number p does not divide both $b-c$ and $b+c$. It follows that either

$$p^n \setminus b - c \quad \text{or} \quad p^n \setminus b + c$$

If $p^n \setminus b - c$, then

$$c \equiv b \text{ (modulo } p^n)$$

On the other hand, if $p^n \setminus b + c$, then

$$c \equiv p^n - b \text{ (modulo } p^n)$$

We conclude that c is not an additional solution, and that either there are two solutions in the range $1, \ldots, p^n - 1$ or there are none. ♢

Cor 6.4.11. *Let p be an odd prime. Then the number of quadratic residues among the numbers $1, \ldots, p-1$ is*

$$\frac{p-1}{2}$$

Proof: Since none of the numbers $1, \ldots, p-1$ is divisible by p, it follows from Theorem 6.4.10 that the mapping

$$x \mapsto x^2 \bmod p$$

from $1, \ldots, p-1$ to itself is two-to-one. Thus, the image of this mapping, i.e., the set of quadratic residues, has cardinality $\frac{p-1}{2}$. ♢

POWER OF 2 AS MODULUS

For modulus 2, the number 1 is the only quadratic residue, and the congruence $x^2 \equiv 1 \bmod 2$ has the unique solution $x = 1$. For modulus 4, the numbers 1 and 3 are relatively prime. The number 1 is a quadratic residue, and the number 3 is a quadratic non-residue. The congruence $x^2 \equiv 1 \bmod 4$ has the two solutions $x = 1$ and $x = 3$. For higher powers of 2, there is the following theorem.

Theorem 6.4.12. *Let n be an integer greater than 2, and let a be a quadratic residue of 2^n, whose smallest positive solution is the number b. Then in the range $1, \ldots, 2^n - 1$, the congruence*

$$x^2 \equiv a \text{ (modulo } 2^n) \qquad (6.4.7)$$

has exactly these four solutions and no others:

$$b, \quad 2^n - b, \quad 2^{n-1} - b, \quad 2^{n-1} + b \tag{6.4.8}$$

Proof: Squaring any of the three other proposed solutions implies immediately that it is a solution to the congruence (6.4.7). It is also clear that the four asserted solutions are mutually non-congruent modulo 2^n.

To see that there are no other possible solutions, consider a number c such that $c^2 \equiv a$ (modulo 2^n). Then, since both b and c satisfy the congruence (6.4.7), it follows that

$$2^n \setminus b^2 - c^2$$

Equivalently,

$$2^n \setminus (b-c)(b+c)$$

It may be asserted that 4 cannot divide both $b-c$ and $b+c$, since otherwise, the number 4 would divide their sum $2b$, from which it would follow that b is even, implying that a is even, contrary to the choice of a. Accordingly, either

$$2^{n-1} \setminus b - c \quad \text{or} \quad 2^{n-1} \setminus b + c \tag{6.4.9}$$

One alternative under (6.4.9) is that $2^{n-1} \setminus b - c$. Then, for some integer k, we have

$$\begin{aligned} b - c &= k2^{n-1} \\ \Rightarrow \qquad c &= b - k2^{n-1} \end{aligned}$$

If k is odd then c is one of the four solutions (6.4.8), since

$$c \equiv 2^{n-1} + b$$

and, similarly, if k is even, then

$$c \equiv 2^n + b$$

The other alternative under (6.4.9) is that $2^{n-1} \setminus b + c$. Then $c = -b + k2^{n-1}$, for some integer k. If k is odd then $c \equiv 2^{n-1} - b$, and if k is even, then $c \equiv 2^n - b$, so it is not a fifth solution.

We conclude that either there are four solutions in the range $1, \ldots, p^n - 1$, as indicated, or there are none. $\diamondsuit$

6.5 EULER PHI-FUNCTION

DEF: The number of positive integers not exceeding n that are relatively prime to n is given by the ***Euler phi-function*** $\phi(n)$.

Here are the first few values of the Euler phi-function:

n	1	2	3	4	5	6	7	8	9	$\cdots$
ϕ_n	1	1	2	2	4	2	6	4	6	$\cdots$

It is particularly easy to evaluate $\phi(n)$ when n is prime.

Proposition 6.5.1. *If the number p is prime, then*

$$\phi(p) \;=\; p-1$$

Conversely, if $\phi(p) \;=\; p-1$, then p is prime.

Proof: Suppose that p is a prime number. Then each of the numbers

$$1, \quad 2, \quad \ldots, \quad p-1$$

is relatively prime to p, which implies that $\phi(p) \;=\; p-1$. Conversely, if p is not a prime number, then at least one of those $p-1$ numbers is not relatively prime to p, which implies that $\phi(p) < p-1$. $\diamondsuit$

In this section, we develop some properties of $\phi(n)$ and give a method of calculating that is much simpler than inclusion-exclusion (see Exercises to §3.6).

Euler's Generalization of Fermat's Thm

Euler generalized Fermat's Theorem:

Theorem 6.5.2 [Euler's Theorem]. *Let b and n be integers with $b \perp n$ and $n > 1$. Then*

$$b^{\phi(n)} \equiv 1 \text{ (modulo } n)$$

Proof: We observe that if modulus n is prime, then the conclusion reduces to Fermat's Thm. More generally, let

$$r_1, \quad r_2, \quad \ldots, \quad r_{\phi(n)}$$

be the set of numbers $\leq n$ and relatively prime to n.

Assertion 1: Each of the numbers

$$br_1, \quad br_2, \quad \ldots, \quad br_{\phi(n)}$$

is relatively prime to the number n.

Proof of Assertion 1: Suppose that p is a prime number that divides n and also divides the product br_j. Then p would divide either b or r_j. Whichever it divides would not be relatively prime to n, a contradiction in either case. ♢ Assertion 1

Assertion 2: If $i \neq j$, then $br_i \not\equiv br_j$ (modulo n).

Proof of Assertion 2: Suppose that $n \setminus b(r_i - r_j)$. Since $n \perp b$, none of the prime divisors of n divides b. It follows that $n \setminus r_i - r_j$. Since $|r_i - r_j| < n$, it follows that $r_i = r_j$, and thus, that $i = j$, a contradiction. ♢ Assertion 2

Asrt 3: $br_1 \cdot br_2 \cdot \cdots \cdot br_{\phi(n)} \equiv r_1 r_2 \cdot \cdots \cdot r_{\phi(n)}$ (modulo n).

Proof of Assertion 3: It follows from Assertions 1 and 2 and the pigeonhole principle that the values

$$br_1 \bmod n, \quad \ldots, \quad br_{\phi(n)} \bmod n$$

are a perm of the values $r_1, \ldots, r_{\phi(n)}$. ◊ Assertion 3

Completion of Proof: Assertion 3 implies that

$$b^{\phi(n)} r_1 r_2 \cdots r_{\phi(n)} \equiv r_1 r_2 \cdots r_{\phi(n)} \text{ (modulo } n)$$

and, in turn, that

$$n \setminus (b^{\phi(n)} - 1)\, r_1 r_2 \cdots r_{\phi(n)}$$

Since each of the numbers r_j is relatively prime to n, it follows that

$$n \setminus (b^{\phi(n)} - 1)$$

Thus, $b^{\phi(n)} \equiv 1$ (modulo n). ◊

Example 6.5.1: The numbers relatively prime to 15 are

$$1,\ 2,\ 4, 7,\ 8,\ 11,\ 13,\ 14$$

Thus, $\phi(15) = 8$. The numbers 4 and 7 are relatively prime to 15. We observe that

$$4^8 \equiv 16^4 \equiv 1^4 \equiv 1 \bmod 15$$
$$7^8 \equiv 49^4 \equiv 4^4 \equiv 16^2 \equiv 1^2 \equiv 1 \bmod 15$$

Evaluating the Phi-Function

Prop 6.5.1 was a first step toward a general formula for $\phi(n)$. We now continue the pursuit of a formula.

Thm 6.5.3. *Let p be a prime number and e a positive integer. Then*

$$\phi(p^e) \;=\; p^e - p^{e-1}$$

Proof: A number is not relatively prime to p^e if and only if it is divisible by p. In the integer interval $[1 : p^e]$, the numbers divisible by p are

$$p, \quad 2p, \quad \ldots, \quad p^{e-1}p$$

The cardinality of the complementary set is $p^e - p^{e-1}$. $\diamondsuit$

Example 6.5.2: If $p = 2$, then the numbers relatively prime to 2^e are the odd numbers less than 2^e. Clearly, there are

$$\frac{2^e}{2} \;=\; 2^e - 2^{e-1}$$

such odd numbers.

DEF: A function $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is a ***multiplicative function*** if whenever $m \perp n$

$$f(mn) \;=\; f(m)f(n)$$

Thm 6.5.4. *The Euler phi-function is multiplicative.*

Proof: Let m and n be integers such that $m \perp n$. Then

$$\begin{aligned}
\phi(mn) &= \sum_{b=0}^{mn-1} (b \perp mn) && \text{(definition of } \phi\text{)} \\
&= \sum_{b=0}^{mn-1} (b \perp m)(b \perp n) && \text{(Theorem A2.2)} \\
&= \sum_{b=0}^{mn-1} (b \bmod m \perp m)(b \bmod n \perp n) && \text{(Prop 6.1.1)} \\
&= \sum_{j=0}^{m-1} \sum_{k=0}^{n-1} (j \bmod m \perp m)(k \bmod n \perp n) && \text{(Thm 6.2.3)} \\
&= \sum_{j=0}^{m-1} (j \bmod m \perp m) \sum_{k=0}^{n-1} (k \bmod n \perp n) \\
&= \phi(m)\,\phi(n) && \diamondsuit
\end{aligned}$$

Example 6.5.3: By sequential testing, we determine that the numbers relatively prime to 36 are

$$1 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 25 \quad 29 \quad 31 \quad 35$$

Thus, $\phi(36) = 12$. Either by sequential testing of the smaller positive integers or by Theorem 6.5.3, we see that $\phi(4) = 2$ and $\phi(9) = 6$, Thus

$$\phi(36) = 12 = 2 \cdot 6 = \phi(4)\phi(9)$$

Theorem 6.5.5. *Let b be a positive integer with the prime power factorization*

$$b \;=\; p_1^{e_1}\cdots p_k^{e_k}$$

Then

$$\phi(b) \;=\; \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1)$$

Proof: This follows immediately from Theorems 6.5.3 and 6.5.4. ♢

Corollary 6.5.6. *Let b be a positive integer with the prime power factorization*

$$b \;=\; p_1^{e_1}\;\cdots\;p_k^{e_k}$$

Then

$$\phi(b) \;=\; b\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

Proof: Starting from Theorem 6.5.5,

$$\begin{aligned}\phi(b) \;&=\; \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1) \;=\; \prod_{i=1}^{k} p_i^{e_i}\left(\frac{p_i-1}{p_i}\right)\\ &=\; \prod_{i=1}^{k} p_i^{e_i}\left(1-\frac{1}{p_i}\right) \;=\; b\cdot\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)\end{aligned} \qquad ♢$$

Example 6.5.4: $60 = 2^2 \cdot 3 \cdot 5$. By Corollary 6.5.6,

$$\begin{aligned} \phi(60) &= 60 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16 \end{aligned}$$

The sixteen numbers relatively prime to 60 are

$$\begin{array}{cccccccc} 1 & 7 & 11 & 13 & 17 & 19 & 23 & 29 \\ 31 & 37 & 41 & 43 & 47 & 49 & 53 & 59 \end{array}$$

By combining Corollary 6.5.6 with Euler's theorem, we can quickly evaluate some otherwise hard-looking congruences.

Example 6.5.5: In reducing each of these congruences of an exponentiated expression, first the base is reduced by dividing by the modulus m, and then the exponent is reduced by dividing by $\phi(m)$.

$$\begin{aligned} 289^{45} \bmod 15 &= 4^{45} \bmod 15 = 4^5 \bmod 15 = 4 \\ 1728^{613} \bmod 35 &= 13^{613} \bmod 35 = 13^{13} \bmod 35 = 13 \\ 1205^{5106} \bmod 21 &= 8^{5106} \bmod 21 = 8^3 \bmod 21 = 8 \end{aligned}$$

Summing Phi over Divisors of n

We are now concerned with proving the following classical result:

$$\sum_{d \,\backslash\, n} \phi(d) = n$$

The proof is most easily understood as a generalization of an example.

Example 6.5.6: The divisors of 12 are

$$d = 1 \quad 2 \quad 3 \quad 4 \quad 6 \quad 12$$

The sum of the values of $\phi(d)$ is

$$\sum_{d \setminus 12} \phi(d) = 1+1+2+2+2+4 = 12$$

This phenomenon can be explained by considering the unreduced fractions of the form $\frac{j}{12}$: for $j = 1, \ldots, 12$

$$\tfrac{1}{12} \quad \tfrac{2}{12} \quad \tfrac{3}{12} \quad \tfrac{4}{12} \quad \tfrac{5}{12} \quad \tfrac{6}{12} \quad \tfrac{7}{12} \quad \tfrac{8}{12} \quad \tfrac{9}{12} \quad \tfrac{10}{12} \quad \tfrac{11}{12} \quad \tfrac{12}{12}$$

First reduce them to

$$\tfrac{1}{12} \quad \tfrac{1}{6} \quad \tfrac{1}{4} \quad \tfrac{1}{3} \quad \tfrac{5}{12} \quad \tfrac{1}{2} \quad \tfrac{7}{12} \quad \tfrac{2}{3} \quad \tfrac{3}{4} \quad \tfrac{5}{6} \quad \tfrac{11}{12} \quad \tfrac{1}{1}$$

and then regroup them according to their denominators

$$\underbrace{\frac{1}{1}}_{1=\phi(1)} \quad \underbrace{\frac{1}{2}}_{1=\phi(2)} \quad \underbrace{\frac{1}{3} \quad \frac{2}{3}}_{2=\phi(3)} \quad \underbrace{\frac{1}{4} \quad \frac{3}{4}}_{2=\phi(4)} \quad \underbrace{\frac{1}{6} \quad \frac{5}{6}}_{2=\phi(6)} \quad \underbrace{\frac{1}{12} \quad \frac{5}{12} \quad \frac{7}{12} \quad \frac{11}{12}}_{4=\phi(12)}$$

The set of numerators in each reduced subgrouping is precisely the set of numbers that are relatively prime to the common denominator of that subgrouping. Thus, the number of fractions in the subgrouping corresponding to the divisor d of 12 equals $\phi(d)$. Since the subgroupings effectively partition the original set of unreduced fractions, it follows that

$$\sum_{d \backslash 12} \phi(d) \;=\; 12$$

Theorem 6.5.7. *Let n be any positive integer. Then*

$$\sum_{d \backslash n} \phi(d) \;=\; n$$

Proof: For each divisor d of n, the value $\phi(d)$ equals the number of unreduced fractions in the set

$$\frac{1}{n} \quad \frac{2}{n} \quad \cdots \quad \frac{n}{n}$$

whose denominator is d after reduction. Since every one of the n unreduced fractions reduces to a unique reduced fraction, the conclusion follows. $\diamondsuit$

Example 6.5.7: The divisors of 15 are

$$d \;=\; 1 \quad 3 \quad 5 \quad 15$$

The sum of the values of $\phi(d)$ is

$$\sum_{d \backslash 15} \phi(d) \;=\; 1 + 2 + 4 + 8 \;=\; 15$$

6.6 THE MÖBIUS FUNCTION

August F. Möbius (1790-1868), a student of Gauss, was later a professor of mathematics at Leipzig, whose most celebrated mathematical association is quite likely with the surface called a Möbius strip, which is one-sided when imbedded in 3-dimensional space. He was also an astronomer. This section concerns one of his contributions to classical number theory, the *Möbius function*, and its use in a summation principle called *Möbius inversion.*

DEF: The ***Möbius function*** $\mu(n)$ is defined recursively on the positive integers as follows:

$$\begin{aligned}\mu(1) &= 1\\ \mu(n) &= -\sum_{d=1}^{n-1}(d\setminus n)\,\mu(d) \quad \text{if } n>1\end{aligned}$$

Example 6.6.1: We consider the smallest cases.

$$\begin{aligned}\mu(2) &= -\mu(1) = -1\\ \mu(3) &= -\mu(1) = -1\\ \mu(4) &= -\mu(1)-\mu(2) = -1-(-1) = 0\\ \mu(5) &= -\mu(1) = -1\\ \mu(6) &= -\mu(1)-\mu(2)-\mu(3) = -1-(-1)-(-1) = 1\\ \mu(7) &= -\mu(1) = -1\end{aligned}$$

$$\begin{aligned}
\mu(8) &= -\mu(1) - \mu(2) - \mu(4) \;=\; -1 - (-1) - 0 \;=\; 0 \\
\mu(9) &= -\mu(1) - \mu(3) \;=\; -1 - (-1) \;=\; 0 \\
\mu(10) &= -\mu(1) - \mu(2) - \mu(5) \;=\; -1 - (-1) - (-1) \;=\; 1 \\
\mu(11) &= -\mu(1) \;=\; -1 \\
\mu(12) &= -\mu(1) - \mu(2) - \mu(3) - \mu(4) - \mu(6) \\
&= -1 - (-1) - (-1) - 0 - 1 \;=\; 0
\end{aligned}$$

We observe that on each of the primes 2, 3, 5, 7, and 11, the value of the Möbius function is -1. It is easy enough to prove that this is true of all primes.

Lemma 6.6.1. *Let p be a prime number. Then*

$$\mu(p) \;=\; -1$$

Proof: Since 1 is the only proper divisor of a prime number p, it follows that

$$\begin{aligned}
\mu(p) &= -\sum_{d=1}^{p-1} (d \setminus p)\, \mu(d) \\
&= -\mu(1) \\
&= -1 \qquad \diamondsuit
\end{aligned}$$

We observe also in Example 6.6.1 that

$$\mu(4) \;=\; \mu(8) \;=\; \mu(9) \;=\; 0$$

and, suspecting that μ is 0-valued on every prime power, we might check a few more and then confirm our hunch.

Example 6.6.1, cont.: We check the next few small cases of prime powers.

$$\begin{aligned}
\mu(16) &= -\mu(1) - \mu(2) - \mu(4) - \mu(8) \;=\; -1 - (-1) - 0 - 0 \;=\; 0 \\
\mu(25) &= -\mu(1) - \mu(5) \;=\; -1 - (-1) \;=\; 0 \\
\mu(27) &= -\mu(1) - \mu(3) - \mu(9) \;=\; -1 - (-1) - 0 \;=\; 0
\end{aligned}$$

Lemma 6.6.2. *Let p^k be a prime power with $k \geq 2$. Then*

$$\mu(p^k) \;=\; 0$$

Proof: Since all the divisors of p^k are of the form p^j, it follows that

$$\mu(p^k) \;=\; -\sum_{j=0}^{k-1} \mu(p^j)$$

Basis: $k = 2$

$$\begin{aligned}
\mu(p^2) &= -\mu(1) - \mu(p) \\
&= -1 - (-1) \\
&= 0
\end{aligned}$$

Ind Step: Assume true for $j = 2, \ldots, k-1$. Then

$$\begin{aligned}
\mu(p^k) &= -\mu(1) - \mu(p) - \mu(p^2) - \ldots - \mu(p^{k-1}) \\
&= -1 - (-1) - 0 - \ldots - 0 \\
&= 0 \qquad\qquad \diamondsuit
\end{aligned}$$

About Multiplicative Functions

It is proved in §6.5 that the Euler function $\phi(n)$ is multiplicative. That is, whenever $m \perp n$

$$\phi(mn) \;=\; \phi(m)\phi(n)$$

In anticipation of calculating the values of the Möbius function, we prove two general theorems about multiplicative functions, after a preparatory lemma.

Lemma 6.6.3. *Let m and n be relatively prime numbers. Then each divisor d of the product mn has a unique representation as the product $d = d_1 d_2$ of a pair of integers d_1 and d_2 such that $d_1 \setminus m$ and $d_2 \setminus n$.*

Proof: By the Fundamental Theorem of Arithmetic, the integer d has a factorization into prime powers, each of which divides either m or n, but not both, since $m \perp n$. The unique representation is

$$d_1 \;=\; \gcd(d, m) \quad \text{and} \quad d_2 \;=\; \gcd(d, n) \qquad \diamondsuit$$

Theorem 6.6.4. *Let $f(n)$ be a function on the positive integers, and let $F(n)$ be the function*

$$F(n) \;=\; \sum_{d \,\setminus\, n} f(d)$$

If $f(n)$ is multiplicative, then so is $F(n)$.

Proof: Let m and n be relatively prime numbers. Then

$$\begin{aligned}
F(m)\,F(n) &= \sum_{d_1\,\backslash\,m} f(d_1) \sum_{d_2\,\backslash\,n} f(d_2) && \text{(definition of } F\text{)} \\
&= \sum_{d_1\,\backslash\,m}\sum_{d_2\,\backslash\,n} f(d_1)\,f(d_2) && \text{(distribution of mult)} \\
&= \sum_{d_1\,\backslash\,m}\sum_{d_2\,\backslash\,n} f(d_1 d_2) && (f \text{ is multiplicative}) \\
&= \sum_{(d_1,d_2)\,:\,d_1\,\backslash\,m \,\wedge\, d_2\,\backslash\,n} f(d_1 d_2) \\
&= \sum_{d\,\backslash\,mn} f(d) && \text{(Lemma 6.6.3)}\diamondsuit
\end{aligned}$$

Example 6.6.2: To illustrate Theorem 6.6.4, let f be a multiplicative function, $m = 10$ and $n = 9$. Then

$$\begin{aligned}
F(90) &= f(1) + f(2) + f(3) + f(5) + f(6) + f(9) \\
&\quad + f(10) + f(15) + f(18) + f(30) + f(45) + f(90) \\
&= f(1\cdot 1) + f(2\cdot 1) + f(1\cdot 3) + f(5\cdot 1) + f(2\cdot 3) \\
&\quad + f(1\cdot 9) + f(10\cdot 1) + f(5\cdot 3) + f(2\cdot 9) + f(10\cdot 3) \\
&\quad + f(5\cdot 9) + f(10\cdot 9) \\
&= f(1)f(1) + f(2)f(1) + f(1)f(3) + f(5)f(1) \\
&\quad + f(2)f(3) + f(1)f(9) + f(10)f(1) + f(5)f(3) \\
&\quad + f(2)f(9) + f(10)f(3) + f(5)f(9) + f(10)f(9) \\
&= [f(1) + f(2) + f(5) + f(10)]\cdot[f(1) + f(3) + f(9)] \\
&= F(10)\,F(9)
\end{aligned}$$

The following theorem inverts the relationship of Theorem 6.6.4. It enables us to prove that the Möbius function μ is multiplicative, which is the key property in establishing a formula for the values of μ.

Theorem 6.6.5. *Let f be any function on the positive integers such that the sum*

$$F(m) \;=\; \sum_{d \,\backslash\, m} f(d)$$

is a multiplicative function. Then f itself is a multiplicative function.

Proof: By induction.

Basis: Since F is multiplicative, it follows that $F(1) = 1$. Thus

$$f(1) \;=\; \sum_{d \,\backslash\, 1} f(d) \;=\; F(1) \;=\; 1$$

Ind Hyp: Assume that $f(mn) = f(m)f(n)$ for $m \perp n$ whenever $mn < s$.

Ind Step: Suppose that $m \perp n$ and that $mn = s$. Then

$$F(mn) \;=\; \sum_{d \,\backslash\, mn} f(d) \;=\; \sum_{b \,\backslash\, m} \; \sum_{c \,\backslash\, n} f(bc)$$

We infer that $b \perp c$ within the double sum, since $b \,\backslash\, m$ and $c \,\backslash\, n$, with $m \perp n$. Thus, by the induction hypothesis, we have

$$\begin{aligned} F(mn) &= \left(\sum_{b \,\backslash\, m} \sum_{c \,\backslash\, n} f(b)f(c) \right) - f(m)f(n) + f(mn) \\ &= \left(\sum_{b \,\backslash\, m} f(b) \sum_{c \,\backslash\, n} f(c) \right) - f(m)f(n) + f(mn) \\ &= F(m)\,F(n) - f(m)f(n) + f(mn) \qquad \text{(def of } F\text{)} \end{aligned}$$

It is given that F is multiplicative, which means that $F(mn) = F(m)F(n)$. It follows that

$$f(mn) = f(m)f(n)$$

Thus, f is multiplicative. ♢

Evaluating Mu

Thm 6.6.6. *The Möbius function μ is multiplicative.*

Proof: Immediately from the definition of μ, the function

$$F(m) = \sum_{d \,\backslash\, m} \mu(d)$$

has the value

$$\begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{otherwise} \end{cases}$$

Thus, the function $F(m)$ is multiplicative. It follows from Theorem 6.6.5 that the function μ is multiplicative. ♢

Thm 6.6.7. *Let $p_1, \ldots, p_r$ be different primes. Then*

$$\mu(p_1^{e_1} \ldots p_r^{e_r}) = \begin{cases} (-1)^r & \text{if } e_1 = \cdots = e_r = 1 \\ 0 & \text{if } e_j \geq 2, \text{ for any } j \end{cases}$$

Proof: This follows from Lemma 6.6.1, Lemma 6.6.2, and the fact that μ is multiplicative. ♢

Example 6.6.3: We use Theorem 6.6.7 to determine some values of $\mu(n)$.

$$\begin{aligned} \mu(1) &= 1 \\ \mu(2) &= -1 \\ \mu(4) &= \mu(2^2) = 0 \\ \mu(6) &= \mu(2 \cdot 3) = (-1)^2 = 1 \\ \mu(12) &= \mu(2^2 \cdot 3) = 0 \\ \mu(30) &= \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1 \\ \mu(210) &= \mu(2 \cdot 3 \cdot 5 \cdot 7) = (-1)^4 = 1 \end{aligned}$$

Möbius Inversion

The following identity facilitates the manipulation of a summation indexed over a lattice of divisors.

Lemma 6.6.8. *Let m and k be positive integers. Then*

$$\left\{\frac{m}{d} : k \backslash d \backslash m\right\} = \left\{\frac{m/k}{c} : c \backslash \frac{m}{k}\right\}$$

Proof: First suppose that $k \backslash d \backslash m$. Take $c = \frac{d}{k}$. Then

$$\frac{m}{d} = \frac{m}{kc} = \frac{m/k}{c} \text{ with } c \backslash \frac{m}{k}$$

Conversely, suppose that $c \backslash \frac{m}{k}$. Take $d = ck$. Then

$$\frac{m/k}{c} = \frac{m/k}{d/k} = \frac{m}{d} \text{ with } k \backslash d \backslash m \qquad \diamondsuit$$

Theorem 6.6.9 [*Möbius Inversion Principle*]. *The integer function F is related to the integer function f by the summation*

$$F(m) = \sum_{d \backslash m} f(d)$$

if and only if the function f is related to the function F by the summation

$$f(m) = \sum_{d \backslash m} \mu\left(\frac{m}{d}\right) F(d)$$

Proof: First suppose that

$$F(m) = \sum_{d \backslash m} f(d)$$

Then

$$\begin{aligned}
\sum_{d \backslash m} \mu\left(\frac{m}{d}\right) F(d) &= \sum_{d \backslash m} \mu\left(\frac{m}{d}\right) \sum_{k \backslash d} f(k) && \text{(subst for } F(d)\text{)} \\
&= \sum_{d \backslash m} \sum_{k \backslash d} \mu\left(\frac{m}{d}\right) f(k) \\
&= \sum_{k \backslash m} \sum_{k \backslash d \backslash m} \mu\left(\frac{m}{d}\right) f(k) && \text{(swap sum order)} \\
&= \sum_{k \backslash m} f(k) \sum_{k \backslash d \backslash m} \mu\left(\frac{m}{d}\right) \\
&= \sum_{k \backslash d} f(k) \sum_{c \backslash \frac{m}{k}} \mu\left(\frac{m/k}{c}\right) && \text{(Lemma 6.6.8)} \\
&= \sum_{k \backslash d} f(k) \left(\frac{m}{k} = 1\right) && \text{(definition of } \mu\text{)} \\
&= \sum_{k \backslash d} f(k)\,(k = m) \\
&= f(m)
\end{aligned}$$

This completes the "forward" direction.

Conversely, suppose that

$$f(m) = \sum_{d \backslash m} \mu\left(\frac{m}{d}\right) F(d)$$

Then

$$\sum_{d \backslash m} f(d) = \sum_{d \backslash m} \sum_{k \backslash d} \mu\left(\frac{d}{k}\right) F(k) \qquad \text{(subst for } f(d)\text{)}$$

$$
\begin{aligned}
&= \sum_{k \setminus d} \sum_{k \setminus d \setminus m} \mu\left(\frac{d}{k}\right) F(k) && \text{(swap sum order)} \\
&= \sum_{k \setminus d} F(k) \sum_{k \setminus d \setminus m} \mu\left(\frac{d}{k}\right) \\
&= \sum_{k \setminus d} F(k) \sum_{k \setminus d \setminus m} \mu\left(\frac{m}{d}\right) && \text{(rearrange summands)} \\
&= \sum_{k \setminus d} F(k) \sum_{c \setminus \frac{m}{k}} \mu\left(\frac{m/k}{c}\right) && \text{(Lemma 6.6.8)} \\
&= \sum_{k \setminus d} F(k) \ \left(\frac{m}{k} = 1\right) && \text{(definition of } \mu) \\
&= \sum_{k \setminus d} F(k) \ (k = m) \\
&= F(m) && \diamondsuit
\end{aligned}
$$

Example 6.6.4: We recall from Theorem 6.5.7 that

$$\sum_{d \setminus n} \phi(d) \ = \ n$$

For $n = 6$, the sum on the left is

$$\phi(1) + \phi(2) + \phi(3) + \phi(6) \ = \ 1 + 1 + 2 + 2 \ = \ 6 \ = \ n$$

According to the Möbius inversion principle, one expects that

$$\phi(6) \ = \ \sum_{d \setminus 6} \mu\left(\frac{6}{d}\right) d$$

The value of this sum is

$$\begin{aligned}\mu(6)\cdot 1 + \mu(3)\cdot 2 + \mu(2)\cdot 3 + \mu(1)\cdot 6 \\ &= 1\cdot 1 + (-1)\cdot 2 + (-1)\cdot 3 + 1\cdot 6 \\ &= 1 - 2 - 3 + 6 \\ &= 2 \\ &= \phi(6)\end{aligned}$$

which serves as empirical confirmation.