Chapter 3: Ancient Greek Number Theory

Exercise 3.6 Prove that if n and m are coprime, then $\sigma(nm) = \sigma(n)\,\sigma(m)$

Proof. Let the prime factorization of nm be $nm = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Being $\gcd(n, m) = 1$, if $p_i \mid n$ then $p_i \not\mid m$ (and viceversa), $1 \leq i \leq k$. In consequence, if the prime factorization of n is $n = q_1^{\beta_1} \dots q_l^{\beta_l}$, then any q_i cannot appear in the prime factorization of m. That is, if the prime factorization of m is $m = r_1^{\gamma_1} \dots r_s^{\gamma_s}$, then $q_i \neq r_j$, $1 \leq i \leq l$, $1 \leq j \leq s$. Thus,

$$\begin{aligned}
\sigma(nm) &= \sigma(p_1^{\alpha_1} \dots p_k^{\alpha_k}) \\
&= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \\
&= \prod_{i=1}^{l} \frac{q_i^{\beta_i+1} - 1}{q_i - 1} \prod_{j=1}^{s} \frac{r_i^{\gamma_i+1} - 1}{r_i - 1} \\
&= \sigma(q_1^{\beta_1} \dots q_l^{\beta_l})\,\sigma(r_1^{\gamma_1} \dots r_s^{\gamma_s}) \\
&= \sigma(n)\,\sigma(m)
\end{aligned}$$

□

Exercise 3.7 Prove that every even perfect number is a triangular number.

Proof. Let k be an even perfect number. Then, by the Euclid-Euler theorem, $k = 2^{n-1}(2^n - 1)$ for some $n \in \mathbb{N}$, where $2^n - 1$ is prime. Thus,

$$\begin{aligned}
k &= 2^{n-1}(2^n - 1) \\
&= (2^n - 1)(2^n/2) \\
&= \frac{(2^n - 1)2^n}{2} \\
&= \triangle_{2^n - 1}
\end{aligned}$$

□

Exercise 3.8 Prove that the sum of the reciprocals of the divisors of a perfect number is always 2.

Proof. Let n be a perfect number with divisors $d_1, \dots, d_k$. By definition of perfect number, we have that

$$\sigma(n) = d_1 + \cdots + d_k = 2n$$

which implies that

$$2 = \frac{d_1 + \cdots + d_k}{n} = \frac{d_1}{n} + \cdots + \frac{d_k}{n}$$

Since $d_i \mid n$, $1 \leq i \leq k$, $n = d_i q_i$. But $q_i \mid n$ as well, and so $q_i = d_j$. Then, $d_i/n = 1/d_j$. In consequence, every summand on the right-hand side of the previous equation can be rewritten as the reciprocal of some divisor of n, and so

$$2 = \frac{d_1}{n} + \cdots + \frac{d_k}{n} = \frac{1}{d_1} + \cdots + \frac{1}{d_k}$$

□

Chapter 4: Euclid's Algorithm

Exercise 4.3 Prove that $\sqrt[3]{16} + \sqrt[3]{54} = \sqrt[3]{250}$

Proof. $16 = 2^4$, $54 = 2 \cdot 3^3$ and $250 = 2 \cdot 5^3$. Then,

$$\begin{aligned} \sqrt[3]{16} + \sqrt[3]{54} &= \sqrt[3]{2^4} + \sqrt[3]{2 \cdot 3^3} \\ &= 2\sqrt[3]{2} + 3\sqrt[3]{2} \\ &= 5\sqrt[3]{2} \\ &= \sqrt[3]{5^3} \cdot \sqrt[3]{2} \\ &= \sqrt[3]{2 \cdot 5^3} \\ &= \sqrt[3]{250} \end{aligned}$$

□

Exercise 4.4 Prove that, for any odd square number x, there is an even square number y such that $x + y$ is a square number.

Proof. Since x is square and odd, there must be an $n \in \mathbb{N}$ such that $x = (2n+1)^2$. Let y be some even square number. Thus, there must be an $m \in \mathbb{N}$ such that $y = (2m)^2$. It follows that

$$\begin{aligned} x + y &= (2n+1)^2 + (2m)^2 \\ &= 4(n^2 + m^2) + 4n + 1 \end{aligned}$$

We must define m as a function of n in such a way that this number conforms a square. In order to do this, let's see what happens for some small cases:

- If $n = 1$, then $x = 9$. If we set $m = 2$, $y = 16$ and $x + y = 25$, which is a square.
- If $n = 2$, then $x = 25$. Taking $m = 6$, $y = 144$ and $x + y = 169$, which is a square (since $13^2 = 169$).
- If $n = 3$, then $x = 49$. Now, m can be 12, and then $y = 576$ and $x + y = 625 = 25^2$.

A careful analysis of these cases reveals a pattern: $m = n^2 + n$. Substituting this in the equation shown before,

$$\begin{aligned} x + y &= 4(n^2 + m^2) + 4n + 1 \\ &= 4(n^2 + (n^2 + n)^2) + 4n + 1 \\ &= 4n^2 + 4(n^2 + n)^2 + 4n + 1 \\ &= 4(n^2 + n)^2 + 4(n^2 + n) + 1 \\ &= (2(n^2 + n) + 1)^2 \end{aligned}$$

□

Exercise 4.5 Prove that, if x and y are both sums of two squares, then so is their product xy.

Proof. Being x and y both sums of two squares, we can write them like so:

$$\begin{aligned} x &= x_1^2 + x_2^2 \\ y &= y_1^2 + y_2^2 \end{aligned}$$

This implies that

$$\begin{aligned} xy &= (x_1^2 + x_2^2)\,(y_1^2 + y_2^2) \\ &= x_1^2 y_1^2 + x_1^2 y_2^2 + x_2^2 y_1^2 + x_2^2 y_2^2 \end{aligned}$$

After several failed attempts at completing the squares (i.e., adding and subtracting the same thing), the following Python script was used to gain some insight into the underlying pattern of xy:

```
def find_squares(x, y):
    x1, x2 = x
    y1, y2 = y
    n = (x1**2 + x2**2)*(y1**2 + y2**2)
    return [(i,j) for i in xrange(n)
                  for j in xrange(i,n)
                  if n == i**2 + j**2]
```

For example,

- `find_squares((2,3), (5,7))` $\to$ `[(1, 31), (11, 29)]`.
- `find_squares((1,2), (3,4))` $\to$ `[(2, 11), (5, 10)]`.

Playing with this script and guessing how to combine the elements in the input tuples in order to generate an output tuple (z_1, z_2), the following pattern emerged:

$$\begin{aligned} z_1 &= x_2y_1 + x_1y_2 \\ z_2 &= x_2y_2 - x_1y_1 \end{aligned}$$

Indeed,

$$\begin{aligned} z_1^2 + z_2^2 &= (x_2y_1 + x_1y_2)^2 + (x_2y_2 - x_1y_1)^2 \\ &= ((x_2y_1)^2 + (x_1y_2)^2 + 2x_2y_1x_1y_2) + ((x_2y_2)^2 + (x_1y_1)^2 - 2x_2y_2x_1y_1) \\ &= x_2^2y_1^2 + x_1^2y_2^2 + x_2^2y_2^2 + x_1^2y_1^2 \\ &= x_1^2y_1^2 + x_1^2y_2^2 + x_2^2y_1^2 + x_2^2y_2^2 \\ &= xy \end{aligned}$$

□

Chapter 5: The Emergence of Modern Number Theory

Exercise 5.1 Prove that if $n > 4$ is composite, then $(n-1)!$ is a multiple of n.

Proof. Let $n > 4$ be a composite integer with prime factorization $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. First note that, if d is a proper divisor of n, then $d \mid (n-1)!$. Indeed, $d \leq n-1$, and so $(n-1)! = (n-1)\cdot(n-2)\cdots d\cdot(d-1)\cdots 1$.

Suppose that $k > 1$. Then, $p_i^{\alpha_i} \mid (n-1)!$, $1 \leq i \leq k$. Since $p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ are pairwise coprime, we have that $n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \mid (n-1)!$.

Now, suppose that $k = 1$. Since n is composite and $n = p_1^{\alpha_1} > 4$, then either $p_1 > 2$ or otherwise $\alpha_1 > 2$. In the latter case, $(n-1)! = (n-1)\cdot(n-2)\cdots p_1^{\alpha_1-1}\cdots p_1\cdots 1$, and so $n = p_1^{\alpha_1} \mid (n-1)!$. Otherwise, if $\alpha_1 = 2$, $2 \cdot p_1 < p_1^2 = n$, and so $(n-1)! = (n-1)\cdot(n-2)\cdots 2p_1\cdots p_1\cdots 1$, which means that $n = p_1^2 \mid (n-1)!$. □

Chapter 6: Abstraction in Mathematics

Exercise 6.3 Prove that any group has at least one element.

Proof. Any group, by definition, has an identity element e. □

Exercise 6.4 What is the order of e? Prove that e is the only element of such order.

Answer. Let G be a group with identity element e. The order of e is 1 given that $e^1 = e$. Suppose that $x \in G$ has also order 1. Then, $x^1 = x = e$. □

Exercise 6.5 Prove that if a is an element of order n, then $a^{-1} = a^{n-1}$.

Proof. We know that $a^n = a\,a^{n-1} = e$. Since inverses are unique, then it must be $a^{-1} = a^{n-1}$. □

Exercise 6.7 Prove that any subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group and S a subgroup of G. Let x be a generator of G, and let $i_0 = \min\{i \leq |G| \,/\, x^i \in S\}$. Consider the element $y = x^{i_0} \in S$, and suppose that its order m is such that $m < |S|$. Then, let $z \in S$ be an element such that $z \neq y^j$. Being x a generator of G, we have that $z = x^{j_0}$ for some j_0. By the division algorithm, we can write j_0 as $j_0 = i_0 q + r$, for some $0 \leq r < i_0$. Then,

$$\begin{aligned} z &= x^{j_0} \\ &= x^{i_0 q + r} \\ &= x^{i_0 q}\, x^r \\ &= (x^{i_0})^q\, x^r \\ &= y^q\, x^r \end{aligned}$$

This implies that $x^r = (y^q)^{-1} z \in S$, but this contradicts the minimality of i_0. Hence, such z cannot exist, which proves that y is a generator of S and, consequently, that S is cyclic. □

Exercise 6.8 Prove that any cyclic group is abelian.

Proof. Let G be a cyclic group, and let x be a generator of G. Given $a, b \in G$, we know that there exist $i, j \in \mathbb{N}$ such that $a = x^i$ and $b = x^j$. Then, using the fact that the group operation is associative and that integer addition commutes,

$$ab = x^i\, x^j = x^{i+j} = x^{j+i} = x^j\, x^i = ba$$

□

Exercise 6.10 Prove that every group of prime order is cyclic.

Proof. Let G be a group such that its order p is prime. Since $p > 1$, there must be at least one element in G whose order is greater than 1. Let x be one such element, and let n be its order. The set $S = \{x^i \,/\, 1 \leq i \leq n\}$ (equipped with G's operation) is a subgroup of G, and so, by Lagrange's theorem, $n = |S| \mid |G| = p$, which implies that $n = p$. Thus, x generates G. □

Chapter 7: Deriving a Generic Algorithm

Exercise 7.1 How many additions are needed to compute `fib0(n)`?

Answer. Let $\alpha(n)$ be the number of additions needed to compute `fib0(n)`. $\alpha(n)$ can be characterized by the following recurrence relation:

$$\alpha(n) = \begin{cases} 0 & \text{if } n \leq 1 \\ 1 + \alpha(n-1) + \alpha(n-2) & \text{if } n \geq 2 \end{cases}$$

It can be shown by induction on n that $\alpha(n) = F_{n+1} - 1$. In fact, if $n \leq 1$, $\alpha(n) = 0 = F_{n+1} - 1$, since by definition $F_1 = F_2 = 1$. For $n \geq 2$,

$$\begin{aligned} \alpha(n) &= 1 + \alpha(n-1) + \alpha(n-2) \\ &= 1 + (F_n - 1) + (F_{n-1} - 1) \\ &= (F_n + F_{n-1}) - 1 \\ &= F_{n+1} - 1 \end{aligned}$$

Thus, the number of additions we seek is $\alpha(n) = F_{n+1} - 1 \in \Theta(\varphi^n)$, where φ is the golden ratio. □

Chapter 11: Permutation Algorithms

Exercise 11.1 Prove *Cayley's theorem*: Any group G is isomorphic to a subgroup of the symmetric group on G, Sym(G).

Proof. For any $a \in G$, consider the following function $F_a : G \to G$:

$$F_a(x) = ax$$

- F_a is one-to-one, since $F_a(x) = ax = ay = F_a(y)$ implies that $x = y$ (left multiplying by a^{-1}).
- F_a is onto: for a given $y \in G$, $F_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y$.

Thus, F_a is a bijection on G, which in turn means that F_a is a permutation of the elements in G. Thus, $S = \{F_a \,/\, a \in G\}$ is a subset of Sym(G). Moreover, S is a subgroup of Sym(G):

- S contains the identity permutation: $F_{e_G}(x) = e_G\, x = x$.
- S is closed by composition: $(F_a \circ F_b)(x) = F_a(F_b(x)) = a(bx) = (ab)x = F_{ab}(x)$.
- S is closed by inverses: $F_a^{-1} = F_{a^{-1}}$, since $(F_a \circ F_{a^{-1}})(x) = a(a^{-1}x) = x$.

Let $\mathcal{F} : G \to S$ be a function defined as follows:

$$\mathcal{F}(a) = F_a$$

Then, $\mathcal{F}$ is a group isomorphism from G to S:

- $\mathcal{F}(ab) = F_{ab} = F_a \circ F_b = \mathcal{F}(a) \circ \mathcal{F}(b)$, using that S is closed by composition.
- $\mathcal{F}$ is one-to-one, since $\mathcal{F}(a) = \mathcal{F}(b)$ implies that $F_a(x) = ax = bx = F_b(x)$, and so $a = b$ after right multiplying by x^{-1}.
- $\mathcal{F}$ is onto, since for a given $F_a \in S$, $\mathcal{F}(a) = F_a$.

□

Exercise 11.2 What is the order of S_n?

Answer. S_n contains every permutation of $\{1, \dots, n\}$. Since there are $n!$ of them, the order of S_n is $n!$. □

Exercise 11.3 Prove that, if $n > 2$, S_n is not abelian.

Proof. Let $P_1 = (2\,1\,3\, \dots\, n)$ and let $P_2 = (3\,1\,2\, \dots\, n)$. Then,

- $P_1 \circ P_2 = (1\,3\,2\, \dots\, n)$, and
- $P_2 \circ P_1 = (3\,2\,1\, \dots\, n)$.

Since $P_1 \circ P_2 \neq P_2 \circ P_1$, S_n is not commutative. □

Exercise 11.9 Prove that if a rotation of n elements has a trivial cycle, then it has n trivial cycles.

Proof. Let ρ be an n by k rotation. That is,

$$\rho = (k \bmod n, k + 1 \bmod n, \dots, k + n - 1 \bmod n)$$

Suppose that ρ has a trivial cycle. This means that there is an $0 \leq i < n$ such that $i = k + i \bmod n \Rightarrow k = 0 \bmod n$. Then,

$$\begin{aligned} \rho &= (0 \bmod n, 1 \bmod n, \dots, n - 1 \bmod n) \\ &= (0, 1, \dots, n - 1) \end{aligned}$$

which means that ρ does not move any element. □

Exercise 11.11 How many assignments does 3-reverse rotate perform?

Answer. Call $\alpha_r(f, m, l)$ the number of assignments we seek. First, let $\sigma(f, l)$ be the number of swaps performed by `reverse`(f, l). Since this function swaps element f with element $l-1$, element $f+1$ with element $l-2$, and so on, we have that

$$\sigma(f, l) = \left\lfloor \frac{l-f}{2} \right\rfloor$$

Then, if we note the number of swaps performed by 3-reverse rotate by $\sigma_r(f, m, l)$,

$$\begin{aligned}
\sigma_r(f, m, l) &= \left\lfloor \frac{m-f}{2} \right\rfloor + \left\lfloor \frac{l-m}{2} \right\rfloor + \left\lfloor \frac{l-f}{2} \right\rfloor \\
&\leq \frac{m-f}{2} + \frac{l-m}{2} + \frac{l-f}{2} \\
&= \frac{(m-f)+(l-m)+(l-f)}{2} \\
&= \frac{2l-2f}{2} \\
&= l-f \\
&= n
\end{aligned}$$

being n the number of elements being rotated. Thus, at most n swaps are performed by 3-reverse rotate (and at least $n-1$, following a similar approach). Since each swap takes three assignments,

$$3(n-1) \leq \alpha_r(f, m, l) \leq 3n$$

□

Chapter 12: Extensions of GCD

Exercise 12.2

1. Prove that an ideal I is closed under subtraction.
2. Prove that I contains 0.

Proof.

1. Let R be the ring such that $I \subseteq R$. We know that the additive inverse of 1, -1, is in R. Let $x \in I$. Thus, $-1x = -x \in I$. Now, let $y \in I$. Then, $y - x = y + (-x) \in I$.
2. The first part of the previous argument shows that I is closed under additive inverses. Thus, given $x \in I$ (at least we have one since I is nonempty), $x + (-x) = x - x = 0 \in I$.

□

Exercise 12.3 Prove that all the elements of a linear combination ideal are divisible by any of the common divisors of a and b.

Proof. Let $I = \{xa + yb \,/\, x, y \in R\}$ be a linear combination ideal, let $e = x_0 a + y_0 b \in I$ and let d be a common divisor of a and b. That is, $a = dq_1$ and $b = dq_2$. Thus,

$$\begin{aligned}
e &= x_0 a + y_0 b \\
&= x_0(dq_1) + y_0(dq_2) \\
&= d(x_0 q_1 + y_0 q_2) \\
&= dq
\end{aligned}$$

In other words, e is divisible by d. □

Exercise 12.4 Prove that any element in a principal ideal is divisible by the principal element.

Proof. Follows immediately from the definition of principal ideal and principal element. □

Exercise 12.5 Using Bézout's identity, prove that if p is prime, then any $0 < a < p$ has multiplicative inverse modulo p.

Proof. Actually, this is an immediate corollary of the invertibility lemma: being p prime, any $0 < a < p$ is such that $\gcd(a, p) = 1$. Thus, there exists an $x \in \mathbb{Z}_p$ such that $ax = xa = 1 \bmod p$. An ad-hoc proof can be done using essentially the same argument that proves the inveritibility lemma. $\square$